

**FIFTH IN A SERIES OF HEARINGS
ON SOCIAL SECURITY NUMBER HIGH-RISK ISSUES**

HEARING
BEFORE THE
SUBCOMMITTEE ON SOCIAL SECURITY
OF THE
COMMITTEE ON WAYS AND MEANS
U.S. HOUSE OF REPRESENTATIVES
ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MARCH 30, 2006

Serial No. 109-62

Printed for the use of the Committee on Ways and Means



U.S. GOVERNMENT PRINTING OFFICE

WASHINGTON : 2006

30-440

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON WAYS AND MEANS

BILL THOMAS, California, *Chairman*

E. CLAY SHAW, JR., Florida
NANCY L. JOHNSON, Connecticut
WALLY HERGER, California
JIM MCCRERY, Louisiana
DAVE CAMP, Michigan
JIM RAMSTAD, Minnesota
JIM NUSSLE, Iowa
SAM JOHNSON, Texas
PHIL ENGLISH, Pennsylvania
J.D. HAYWORTH, Arizona
JERRY WELLER, Illinois
KENNY C. HULSHOF, Missouri
RON LEWIS, Kentucky
MARK FOLEY, Florida
KEVIN BRADY, Texas
THOMAS M. REYNOLDS, New York
PAUL RYAN, Wisconsin
ERIC CANTOR, Virginia
JOHN LINDER, Georgia
BOB BEAUPREZ, Colorado
MELISSA A. HART, Pennsylvania
CHRIS CHOCOLA, Indiana
DEVIN NUNES, California

CHARLES B. RANGEL, New York
FORTNEY PETE STARK, California
SANDER M. LEVIN, Michigan
BENJAMIN L. CARDIN, Maryland
JIM MCDERMOTT, Washington
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
MICHAEL R. MCNULTY, New York
WILLIAM J. JEFFERSON, Louisiana
JOHN S. TANNER, Tennessee
XAVIER BECERRA, California
LLOYD DOGETT, Texas
EARL POMEROY, North Dakota
STEPHANIE TUBBS JONES, Ohio
MIKE THOMPSON, California
JOHN B. LARSON, Connecticut
RAHM EMANUEL, Illinois

ALLISON H. GILES, *Chief of Staff*
JANICE MAYS, *Minority Chief Counsel*

SUBCOMMITTEE ON SOCIAL SECURITY

JIM MCCRERY, Louisiana, *Chairman*

E. CLAY SHAW JR., Florida
SAM JOHNSON, Texas
J.D. HAYWORTH, Arizona
KENNY C. HULSHOF, Missouri
RON LEWIS, Kentucky
KEVIN BRADY, Texas
PAUL RYAN, Wisconsin

SANDER M. LEVIN, Michigan
EARL POMEROY, North Dakota
XAVIER BECERRA, California
STEPHANIE TUBBS JONES, Ohio
RICHARD E. NEAL, Massachusetts

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Ways and Means are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

	Page
Advisory of March 23, 2006 announcing the hearing	2

WITNESSES

The Honorable David Dreier, a Representative in Congress from the State of California	5
The Honorable Silvestre Reyes, a Representative in Congress from the State of Texas	9

Federal Trade Commission, Joel Winston, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection	28
U.S. Government Accountability Office, Cynthia M. Fagnoni, Managing Director, Education, Workforce, and Income Security	17

BITS Fraud Reduction Steering Committee, Erik Stein	60
Consumer Data Industry Association, Stuart K. Pratt	68
Council of State Court Administrators, Mary C. McQueen	47
Identity Theft Resource Center, Nicole Robinson	42
National Council of Investigation and Security Services, Bruce Hulme	76

SUBMISSIONS FOR THE RECORD

Kenney, John P., Corona Del Mar, CA, letter	89
Sybesma, Jamie, Fishers, IN, statement	89

CMS Library
C2-07-13
7500 Security Blvd.
Baltimore, Maryland 21244

RECEIVED
JAN 10 1964
U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C.

**FIFTH IN A SERIES OF HEARINGS ON
SOCIAL SECURITY NUMBER HIGH-RISK ISSUES**

THURSDAY, MARCH 30, 2006

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON SOCIAL SECURITY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:40 p.m., in room B-318, Rayburn House Office Building, Hon. Jim McCrery (Chairman of the Subcommittee) presiding.

[The advisory announcing the hearing follows:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE

March 23, 2006

No. SS-14

CONTACT: (202) 225-9263

McCrery Announces Fifth in Series of Subcommittee Hearings on Social Security Number High-Risk Issues

Congressman Jim McCrery, (R-LA), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee will hold the fifth in a series of Subcommittee hearings on Social Security number (SSN) high-risk issues. The hearing will examine the role of SSNs in identity theft and options to enhance SSN privacy. **The hearing will take place on Thursday, March 30, 2006, in room B-318 Rayburn House Office Building, beginning at 2:00 p.m.**

In view of the limited time available to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Subcommittee and for inclusion in the printed record of the hearing.

BACKGROUND:

Identity theft is a serious crime in which a victim's personal information may be used to fraudulently obtain credit, goods or services, employment, government documents or benefits, or to commit other crimes. According to a 2006 survey released by the Council of Better Business Bureaus and Javelin Strategy & Research, there are almost 9 million adult victims of identity fraud (about 4 percent of the U.S. adult population). These victims may spend significant amounts of money and time to resolve their problems: on average \$422 and 40 hours per victim. Total identity theft costs exceed \$50 billion annually.

Although SSNs have many important legitimate uses, the Federal Trade Commission (FTC) indicates that they also play a pivotal role in identity theft. According to the FTC, the SSN is integral to many business transactions, and identity thieves use the SSN as a key to unlock access to the financial benefits of their victims. Despite its vital role in our financial system, there is no Federal law that requires comprehensive confidentiality protection for the SSN. An SSN may be on display to the general public on employee badges, in court documents, or on the Internet. However, there are laws that provide limited SSN confidentiality. For example, the Gramm-Leach-Bliley Act (P.L. 106-102) restricts the reuse and redisclosure of certain personal information, including SSNs, by financial institutions. Also, many States have enacted legislation to restrict the use, disclosure, or display of SSNs.

Members of Congress, concerned about the magnitude of the problem and its devastating effects on victims, have introduced legislation that would place various restrictions and prohibitions on the use, sale, purchase, or display of SSNs, as well as create new criminal and civil penalties for those who misuse SSNs. Also, legislation has been introduced that would require improvements to the process of issuing SSNs or the design of the SSN card to prevent individuals from fraudulently obtaining an SSN or counterfeiting SSN cards.

In announcing the hearing, Chairman McCrery stated, "We must carefully examine all options to keep Social Security numbers, or SSNs, out of the hands of identity thieves. As we do so, we must remember that SSNs play a key role in our soci-

ety, whether in business transactions, tax administration, public benefits, or the court systems. Through this hearing we will explore how best to achieve the appropriate balance between the need for protecting SSN privacy and allowing their use for legitimate and necessary purposes.”

FOCUS OF THE HEARING:

The Subcommittee will examine the role of SSNs in abetting identity theft, and the effects of proposals to prohibit or restrict the use, sale, purchase, or display of SSNs by individuals, businesses, or the government.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Any person(s) and/or organization(s) wishing to submit for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, <http://waysandmeans.house.gov>, select “109th Congress” from the menu entitled, “Hearing Archives” (<http://waysandmeans.house.gov/Hearings.asp?congress=17>). Select the hearing for which you would like to submit, and click on the link entitled, “Click here to provide a submission for the record.” Once you have followed the on-line instructions, completing all informational forms and clicking “submit” on the final page, an email will be sent to the address which you supply confirming your interest in providing a submission for the record. You **MUST REPLY** to the email and **ATTACH** your submission as a Word or WordPerfect document, in compliance with the formatting requirements listed below, by close of business Thursday, April 13, 2006. **Finally**, please note that due to the change in House mail policy, the U.S. Capitol Police will refuse sealed-package deliveries to all House Office Buildings. For questions, or if you encounter technical problems, please call (202) 225-1721.

FORMATTING REQUIREMENTS:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission, but we reserve the right to format it according to our guidelines. Any submission provided to the Committee by a witness, any supplementary materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission or supplementary item not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. All submissions and supplementary materials must be provided in Word or WordPerfect format and MUST NOT exceed a total of 10 pages, including attachments. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record.

2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material not meeting these specifications will be maintained in the Committee files for review and use by the Committee.

3. All submissions must include a list of all clients, persons, and/or organizations on whose behalf the witness appears. A supplemental sheet must accompany each submission listing the name, company, address, telephone and fax numbers of each witness.

Note: All Committee advisories and news releases are available on the World Wide Web at <http://waysandmeans.house.gov>.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202-225-1721 or 202-226-3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Chairman MCCRERY. The Subcommittee hearing will come to order. Good afternoon, everybody. Welcome to our fifth in a series

of hearings on high-risk issues related to Social Security numbers (SSNs). Today, we will examine the use of SSNs by government agencies, businesses, and others, as well as explore options for improving the confidentiality of SSNs.

For many years, this Subcommittee has worked to protect SSN privacy. For example, the Committee on Ways and Means approved bills in the 108th and 106th Congresses that were introduced by my predecessor, Subcommittee Chairman Clay Shaw. Some of the provisions from Mr. Shaw's bill in the 108th Congress have become law, including limits on replacement SSN cards and a prohibition on the display of SSNs on drivers' licenses.

The SSN plays a key role in both our government and in our economy. Since the SSN is a unique number for each person and is widely used, it helps link records at all levels. This, in turn, facilitates administration of government services and benefits, business transactions, and fraud prevention. However, once this essential piece of information is in the hands of identity thieves, it opens a Pandora's box of problems. Stolen SSNs can damage lives and businesses' bottom lines.

Today, we will hear about the current patchwork of Federal and State laws that provide limited and inconsistent confidentiality protection for SSNs. For example, financial institutions are restricted in their ability to release SSN information, but SSNs may appear in any number of publicly available government records, such as court records or property ownership records.

Computers and the Internet have enabled unprecedented information sharing, and anyone who collects, uses, or shares SSN information has a responsibility to protect its confidentiality. Today, we will hear about some of the voluntary steps that government agencies, businesses, and others are taking to protect SSNs from unauthorized disclosure. We also will have the opportunity to explore options for improving SSN protections.

These options involve complicated trade-offs. In some cases, Federal laws and regulations require the collection of SSNs to achieve certain goals, such as efficient and accurate tax administration, child support enforcement, and identification of money launderers and terrorists. As we examine alternatives for improving SSN privacy to help prevent identity theft, we must consider the potential effect on the attainment of those goals. We must also be mindful of the costs that individuals, businesses, and government agencies may incur as a result.

By carefully examining all options to keep SSNs out of the hands of identity thieves and by listening to as many stakeholders as possible, we seek a balance between protecting SSN privacy and allowing its use for legitimate and necessary purposes. Mr. Levin?

Mr. LEVIN. Mr. Chairman, since I basically agree with your opening statement and since both of our colleagues here, I would simply ask that my opening statement be placed in the record.

Chairman MCCRERY. Without objection. Thank you, Mr. Levin.
[The prepared statement of Mr. Levin follows:]

Opening Statement of The Honorable Sander M. Levin, a Representative in Congress from the State of Michigan

The problem of identity theft is serious and growing, claiming almost 9 million victims and costing our economy an estimated \$50 billion a year. The issue within

our Committee's jurisdiction—protecting the Social Security Number—is just one piece of a total strategy to address identity theft, but it is an important one. Government agencies and the private sector must both do their part to prevent and detect identity theft.

When it comes to the Social Security number, the critical issue is striking the right balance between allowing beneficial uses of the number and protecting privacy for individuals. The rapid advance in technology in recent years has greatly aggravated the problem of identity theft. Identity thieves no longer have to rifle through people's trash in search of private information. They increasingly obtain this information by tapping into computer databases and other high-tech means.

Given the evolving nature of the problem, there is a clear need for ongoing oversight. I look forward to hearing more about the issues and options from our witnesses.

In the past, our Subcommittee has been able to work to find this balance in a genuinely bipartisan way, with Republicans and Democrats sitting across the table and coming to agreement on the issues. I hope we will be able to continue in that tradition, and work closely together to act on the information we receive today.

Chairman MCCRERY. Our first panel today is composed of two distinguished colleagues, Mr. Dreier and Mr. Reyes, each of whom have expressed an interest in the issues that this Subcommittee has been exploring for some time now. They were supposed to be here last time, but we had a series of votes, and in an effort to not prolong the necessity for other witnesses to stay, we asked these two colleagues if they could come today, and they graciously agreed to do that.

Welcome, gentlemen. We are interested in your views on this subject. We would like for you to try to summarize those views in about 5 minutes, and we will start with my colleague from California, Mr. Dreier.

STATEMENT OF DAVID DREIER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. DREIER. Thank you very much, Mr. Chairman. Let me begin by expressing my appreciation to you for the hard work that you do in dealing with this issue of Social Security and the specific issue you are tackling right now, and to Mr. Levin and Mr. Johnson and Mr. Brady, I thank all of you for being here. I know we have completed our votes on the floor, but this is a very important issue.

Mr. Reyes and I have come together in a bipartisan way to deal with an issue that is getting a great deal of attention. The issue is immigration reform and border security. I don't know if any of you all recall that we dealt with that back in December and our colleagues in the other body are tackling that question right now, as to how they move ahead this week and next on this issue.

Virtually everything that we do focuses on the supply side of the immigration problem. On border security, what is it that we did? Well, we talked about building a 700-mile wall. We talked about dramatically increasing the size of the Border Patrol, a lot of things that are designed to stem the flow of people coming into this country illegally.

What is it that we really haven't done? We haven't spent much time and effort looking at why it is that they come to the United States of America. That is why Mr. Reyes and I, with the encouragement of T.J. Bonner, who is the President of the National Bor-

der Patrol Council, which is the union of Border Patrol agents, said, let us not just look at the supply side. Let us focus on the demand side here.

Why is it that people come into this country illegally? They come here, 98 percent of them, for one reason and one reason only. They come here looking for a job. They are looking to feed their families. They are looking for economic opportunity. We all know that. Of the 12 million people who are in this country illegally, we know that nearly all of them are here as productive members of society, working, paying taxes, doing things that need to be done in this country.

We know that they are here illegally and there is a strong sense that we need to take action. We need to take action to deal with it.

Right now, there are 94 different combinations of documents, including that flimsy little Social Security card that was first put into place in 1935, that has not been updated once since 1935, that are used for a potential employee to go to a potential employer and get a job—94 different combinations of documents, including a school ID card, a library card. What Mr. Reyes and I have come together to do is very simply to say, why don't we make an attempt to put into place a smart, counterfeit-proof Social Security card with an algorithm strip on the back of it, an algorithm strip which would simply go in and look at the data that is already there. No new data—the government would not get its hands on any new data at all.

This counterfeit-proof card—actually, I carry a counterfeit example of my counterfeit-proof card, this is an old Union 76 credit card and I have just put the Social Security on the top of the card. I used T.J. Bonner's picture, since this was his idea, and his photo is here, and you would have an algorithm strip on the back.

Someone is going in, Mr. Chairman, to look for a job. The potential employer decides, I might want to hire this person. They either swipe this card or call an 800 number. They dial the 800 number and it goes into a databank which is simply taking the SSN, linking it with the U.S. Department of Homeland Security (DHS), and the only information that would go out is yea or nay. Is this person a qualified worker or not a qualified worker?

We put on the bottom of this that this is not a national ID card. I know that from testimony you all have had in the past, from your last hearing, I understood that real concern is raised about if it looks like a duck, walks like a duck, acts like a duck, talks like a duck, it may be a duck. The fact is, this is not a national ID card. Why? The only utilization of this card will be for, number one, Social Security purposes, which are correct, and number two, applying for a new job.

Now, as I look around this room, I feel pretty sanguine that everybody here, including Xavier Becerra, will be reelected as they head toward this November election.

Mr. BECERRA. Is that an endorsement?

Mr. DREIER. You don't want my endorsement, Xavier.

[Laughter.]

That might jeopardize it, if you had my endorsement. The fact is, only people looking, Mr. Chairman, for a new job would be re-

quired to carry this. A senior citizen would never have to have a counterfeit-proof Social Security card. Someone who is a small business man or woman would never have to have a counterfeit-proof Social Security card.

What we have got is we have got a situation where the magnet that draws people across the border is jobs, and if the thumbs-down comes from this card from the databank that is already there, we in our legislation increase the penalty dramatically and we increase enforcement dramatically. By 400 percent, we increase the penalty, from \$10,000 to \$50,000 for hiring, and we have a 5 year prison term, and we also increase by 10,000 the number of enforcement agents.

Now, you and I were talking yesterday about this and I know that everyone in this room pays their taxes simply because they are patriotic Americans, but there may be some people out there who realize that the Internal Revenue Service (IRS) is there and that may be the reason that as April 15 approaches, they will be paying their taxes. I know none of us are among those.

Similarly, if we were to see four or five high-profile arrests due to people who were knowingly hiring those who are here illegally, I am convinced that we would see a great diminution of the number of hirings taking place. I am convinced that we have, if not the panacea, we have the ability to look at what deals with 98 percent of the people who come here illegally to help us address this issue.

Mr. Chairman, I think we have got a great opportunity to do something here and I am pleased that Members of the Hispanic Caucus have joined. Again, it is a very, very bipartisan measure. It is my hope that as we look at the issue of immigration reform, we will be able to recognize that this is better for the employer, easier for the businessman or woman who is looking to hire someone, because they don't have to look at 94 different combinations of documents and they are free of responsibility once they have gotten a yea or nay on it. It is going to help us deal with this very serious problem that we have of illegal immigration and finally see the Social Security Administration (SSA) bring that flimsy little paper to which I was referring into the 21st century.

Thank you very much.

Chairman MCCRERY. Thank you, Mr. Dreier.

[The prepared statement of Mr. Dreier follows:]

**Statement of The Honorable David Dreier, a Representative in Congress
from the State of California**

Chairman McCrery, Ranking Member Levin, Members of the Subcommittee, thank you for providing this opportunity to appear before the Subcommittee's hearing on Social Security high risk issues. Specifically, I would like to discuss the merits of legislation I authored with my friend from El Paso, Mr. Reyes, H.R. 98, the Illegal Immigration Enforcement and Social Security Protection Act, and how it would help to crack down on the hiring of illegal immigrants and curb abuse of the Social Security number and card. I have submitted testimony for the record to two of your previous hearings on this matter, so I'll keep my statement somewhat brief. I want to have ample time to answer your questions.

As I mentioned in previous written testimony, there are 94 different combinations of documents on the current I-9 form that can be used to establish identity and employment eligibility. The Social Security card is one such document. Because the process by which job seekers prove their employment eligibility is so unwieldy and complicated, it plays right into the hands of illegal immigrants who can obtain or copy Social Security numbers and cards. In fact, easy employment powers the job-

magnet that draws people to illegally enter our country. That is why Mr. Reyes and I authored H.R. 98. We need to address the "demand-side" of the illegal immigration issue.

H.R. 98 makes the Social Security card fraud-proof and provides employers with a tamper-free tool to verify work authorization status. This will come as a great relief to employers who have been forced to act as immigration and document experts. Under the bill, the Social Security Administration (SSA) is required to issue cards that contain a digitized photo of the cardholder, as well as other countermeasures to reduce fraud. This includes replacing the flimsy Social Security banknote paper with a durable plastic or similar material. Also, each card will contain physical security features designed to prevent tampering, counterfeiting or duplication.

In addition, this card will have an electronic signature strip that contains an encrypted electronic identification code unique to that individual. Employers could verify worker eligibility via a Department of Homeland Security (DHS) database by swiping the card through an electronic card-reader or simply calling a toll-free number. The employer would know instantaneously whether or not they were permitted to hire the individual in question. As my colleagues on the Subcommittee know, the House-approved border control bill directs SSA to study the implementation and feasibility of such a proposal.

I understand that privacy concerns have been raised regarding H.R. 98; that the bill would create a national ID card. Let me just say unequivocally that H.R. 98 does not create a national ID card. In fact, section 11 of the bill unconditionally prohibits the use of the Social Security card as a national ID card. Let us not forget that job applicants, under current law, are already required to show documents that establish their identity and employment eligibility. Many, if not most, choose to show their employer the combination of a photo ID and their Social Security card. Eliminating a step by actually placing the photo on the Social Security card itself doesn't take us any further down the road of creating a national ID card.

The only time anyone would actually be required to carry the improved Social Security card would either be for Social Security purposes or when they are applying for a new job. H.R. 98 explicitly states that individuals cannot be required to carry the new card, except for these two purposes. And the card itself will contain a disclaimer stating: "This card not to be used for the purpose of identification." Social Security cards had a similar disclaimer from 1946 to 1972.

I also understand that concerns have been raised regarding the privacy and security of the employment eligibility database created under H.R. 98. Let me just say that no one is more sensitive to concerns about privacy and data security than I am. But let's remember, I wouldn't be sitting here in front of you today if we were already doing a great job of securing our Social Security and immigration systems. Nonetheless, we have taken great care to ensure the integrity of the Employment Eligibility Database which H.R. 98 creates. Specifically, the bill prohibits the use of any information in the database by any DHS employee for any purpose other than administering the database, and it requires DHS to limit access to the database to only those employees who administer the database.

We also need to keep in mind that the government already has the information that would be contained on this new Social Security card. An individual's eligibility to work under the law is dependent on whether they are a U.S. citizen, and if not, their immigration status. SSA already maintains citizenship and immigration status files for each worker issued a Social Security card, and our legislation would not require them to gather any additional information than they do currently.

The only thing H.R. 98 does is allow the information that SSA already collects to be used for the purpose of verifying a prospective employee's eligibility to work—via the DHS database—and the authenticity of their Social Security card. This streamlines two separate pre-existing government functions; determining a person's eligibility to work and ensuring that employers do not hire anyone ineligible to work.

Mr. Chairman, in recent years, we have improved the security of almost every government-issued document, passports, green cards, driver's licenses, save one—the Social Security card. With over five million cards issued annually, we need to realize that it's time to bring the Social Security card into the 21st Century. In the process, we will end the magnet of jobs for illegal immigrants.

I believe that H.R. 98 represents an excellent starting point to secure the Social Security card and enhance our efforts to stop the hiring of illegal immigrants. I look forward to working with the Members of the Subcommittee to reach these important goals.

Chairman MCCRERY. Now, our colleague from Texas, Mr. Reyes.

STATEMENT OF SILVESTRE REYES, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. REYES. Thank you, Mr. Chairman, Mr. Levin, fellow colleagues. I am pleased to be here with my good friend and colleague from California, and I just want to make three points, but before I make those points, I want to tell you that in 1986, when the Immigration Control and Reform Act (P.L. 99-603) (IRCA) was passed, it had a provision for employer sanctions in there. Had Congress provided the resources to INS, Border Patrol back then, we wouldn't be having the debates that we are having today.

Fast forward to 2006 and the three points that I want to make are that, as my colleague stated, the technology has gotten to the point where we feel very confident that a Social Security card with biometrics and algorithm and all the other things that have been mentioned were included, it would be safe to say—I always hesitate from the law enforcement background that something is counterfeit-proof, but it would be very hard to replicate with the kind of technology that is available today. You need that card that would, in essence, relieve any employer from the responsibility of having to look at and file as many as nine and ten documents, as the I-9 provision currently requires, with the fraud-proof Social Security card.

The second point I want to make is that along with that card, you need a system, a system where an employer, once he is presented with that card, can check and verify whether it is the individual. If there is a question, they can ask somebody to come out and check it out or maybe check it out through the computer. Those systems exist today. They are not cheap, but I would say they are a lot cheaper than all of these other proposals that have been—and not as controversial as the ones that have been proposed in the bill that we passed in December, the wall, taking citizenship, all these things that are very contentious.

The third point I want to make is that adequate resources must be provided along with it. No system is good if you don't provide the resources for checks. You have got to provide the money. You have got to provide the people. Our bill does that.

Those are the three basic points I wanted to make. I have a statement that I would like to include into the record, but now, being respectful of your time, I will yield back the balance of my time, subject to any questions you might have for me or for my colleague.

Chairman MCCRERY. Thank you, Mr. Reyes.

[The prepared statement of Mr. Reyes follows:]

Statement of The Honorable Silvestre Reyes, a Representative in Congress from the State of Texas

Good afternoon. I would like to thank Chairman Jim McCreery and Ranking Member Sander Levin for giving me the opportunity to testify before this Subcommittee today about the role a new, improved Social Security card could play in allowing employers to determine whether prospective employees are authorized to work in the United States and, ultimately, in helping to curb illegal immigration.

I believe I come to this hearing with a somewhat unique perspective on this important issue. My district of El Paso, Texas—along with its sister city, Ciudad

Júrez, Mexico—comprise the largest metropolitan area on the United States-Mexico border. Also, prior to coming to Congress, I was in the United States Border Patrol for 26½ years. I served as Chief, first in the McAllen sector and subsequently in the El Paso sector from 1984 until my retirement in 1995. I have also done my share of interior immigration enforcement at work sites where undocumented aliens were employed.

As the only Member of Congress with a background in immigration and experience defending our nation's borders, I have firsthand knowledge of what we need to do to reduce illegal immigration and help keep America safe. I have witnessed the difference that strong enforcement of employment laws can make in discouraging attempted illegal entries into the United States. Furthermore, I believe that a fraud-proof Social Security card, coupled with a computerized employment eligibility verification system and properly enforced employer sanctions, could be a critical part of that effort.

In 1986, Congress passed the Immigration Reform and Control Act, which included new sanctions against employers who hire illegal immigrants. After that law was enacted, in parts of the country such as the border region where those of us in law enforcement had the resources to enforce those sanctions, we saw a significant decrease in the number of people trying to enter the country unlawfully. Clearly, once word got out that employers would not hire illegal immigrants, a major incentive to enter the United States was greatly reduced and attempted entries dropped off considerably.

I have been pleased to work with my friend and colleague from California, Rep. David Dreier, on H.R. 98, the Illegal Immigration Enforcement and Social Security Protection Act of 2005. The bill would substantially expand and improve on the 1986 provisions by enhancing the security of Social Security cards and allowing employers to instantaneously verify a prospective employee's eligibility to work in the United States. The bill would also increase civil and criminal penalties for employers who hire illegal immigrants or fail to verify their employment eligibility.

If properly funded and with appropriate oversight and privacy protections, H.R. 98 would be an important step toward halting the flow of people seeking to enter the United States illegally in order to find employment. By doing so, our immigration and border security personnel will be able to focus more of their time, effort, and resources on those who may be trying to enter the country to do us harm.

As you continue to hold hearings on important Social Security matters, I encourage this Subcommittee to consider how a next-generation Social Security card and employment eligibility system could help address some of the urgent immigration matters we face in this country.

Again, thank you for allowing me to testify today, and I look forward to continuing to work with my colleagues on this important issue.

Chairman MCCRERY. Both of your statements will be included in the record. Your written statements will be included in the record in their entirety.

Mr. Dreier, you said the employer would either swipe the card or call an 800 number. Explain that. What 800 number would they call?

Mr. DREIER. Basically, what that would mean is that there would be a databank, the information, again, that the government already has, known information. Is someone an American citizen? Are they here on an H-2A visa, which is basically a farmworker visa, some other kind of work permit? They would simply be told yes or no. This person who is applying for a job to work in your company is, in fact, a qualified worker, and—

Chairman MCCRERY. If you are an employer and you call this 800 number, what do you say?

Mr. DREIER. What you do is you provide the information that is there, the SSN, and obviously the goal would be to have a swipe for people so that they would be able to utilize the algorithm strip. There would be a transition period, clearly, through which they would go that would—obviously, a big challenge—

Mr. REYES. Mr. Chairman, if I can just add to that, if you don't mind—

Chairman MCCRERY. Sure.

Mr. REYES. What happens today when you go into a restaurant or you go into a shop and you pay with a credit card, they put it into the system. They swipe it or they insert it in the machine-readable system. If there is an issue or a problem that they think it may not be you or some other thing, then the merchant will call an 800 number and they will verify the account and all these other things.

That is what we have in mind here. Remember, we are talking about employers, employers that are already used to, by and large, as every American is, in utilizing this kind of a system. It won't be exactly a system like the ATM or the credit card system, but it will be similar, with the card sufficing as proof that it is the individual, that it was presented to the employer, and the employer, in fact, verified it. Any other questions in there about that, there is an 800 number. They pick up the phone, they call and they talk to either a call center or a DHS system that would answer any questions and, again, would relieve the employer of the liability because they have gone and made a good faith effort.

Chairman MCCRERY. I was just trying to get to the question of why the need for a tamper-proof card. If all you need is the number and you can call an 800 number, it seems to me you would need the card—

Mr. DREIER. Well, I think as Mr. Reyes says, it really would be designed as a back-up to deal with—

Chairman MCCRERY. With questions?

Mr. DREIER. —because the goal is to really utilize this algorithm strip that is there that is—

Chairman MCCRERY. Yes.

Mr. DREIER. —again, and I think that Silver is right on target when he says that the notion of saying that something is 100 percent absolutely counterfeit-proof is a bit of a stretch, but there has been no attempt since 1935 to really move the Social Security card itself into the modern era, and I think that we ought to at least engage in the fight, trying to put into place the most technologically advanced mechanism we possibly can to deal with this.

Chairman MCCRERY. Would you put a picture on the—

Mr. DREIER. Yes, it has a photograph on it.

Chairman MCCRERY. It has a photograph on the card, so that would be—

Mr. DREIER. When a person becomes of working age—I know that some people have raised this question, well, would you put the baby picture on, because people get their Social Security card. It is when in their State they would become of working age that the photo-embedded item would be provided on there.

Chairman MCCRERY. Okay. Mr. Levin?

Mr. LEVIN. I am tempted to ask a question, but I think it involves larger issues. For example, what would happen to the people of working age, the 12 million who are here now illegally?

Mr. DREIER. Well, I am happy to answer that question. I think that part of the goal here is that since we are focusing on this question, if 98 percent of the people who come here illegally are

coming to get a job, and with a tamper-proof, smart, counterfeit-proof, whatever you want to call it, Social Security card, they can't get a job, my sense is that many of them might choose to return to a country of origin. I am not saying that absolutely everyone, but I am convinced that would go a long way toward dealing with this overall sweeping problem that we are dealing with of our border security and the problem of illegal immigration.

Mr. LEVIN. I guess my question does open up a larger issue, so we will leave it for another day since the Senate is kind of monopolizing discussion at the moment.

Mr. DREIER. That is why we should weigh in over here a little bit this week on it.

Mr. LEVIN. Okay. Thank you.

Chairman MCCRERY. Well, obviously, if we went to a guest worker program of some sort, then that would facilitate getting something like this—

Mr. DREIER. Oh, absolutely.

Chairman MCCRERY. —that could be used for—

Mr. DREIER. I will say that I believe that as we do this, it is imperative that we have a responsible, non-amnesty-granting temporary worker program that does go hand-in-hand with this so that we can meet the economic demand that exists in this country and then tackle the question that you correctly raise.

Mr. REYES. If I can just—

Chairman MCCRERY. Please.

Mr. REYES. We come together on offering this as one part of the solution, but I do believe that we have got to have comprehensive immigration reform. We have got to have secure borders. We have got to have a guest worker program, which this would fit in with. Then you have got to take care of, as Congressman Levin said, you have got to take care of those people that have been in this country, paying their taxes, being part of our community. That is what I think would be a realistic way to implement this.

What this does is it becomes part of the mechanism of making sure that we don't have the magnet—I can tell you from personal experience, after IRCA, we saw a dramatic downturn in attempted illegal entries for about 3 years. Some areas of our border—I was chief in McAllen at the time with Border Patrol—some areas of our border saw a decline in attempted entries into this country of as much as 80 percent. The reason for that was the publicity that was generated that, for the first time, there were employer sanctions in place. You would not be able to get a job. The attraction of undergoing that arduous trip through the border and trying to get a job somewhere in this country was gone.

It wasn't until about 3 years into the program that people started realizing, well, Congress didn't allot the personnel to check, so my uncle or my cousin or my friend said that if you can make it to Denver, you can still get a job. Even though it had the requirements of the I-9, there were no teeth in the law.

I think that this on its own probably is not the whole solution, but it gets us part of the way, and then comprehensive immigration reform, I think would take us the rest of the way.

Mr. DREIER. Mr. Chairman, what this really does is, again, as we look at this question, why is it that people come into this coun-

try illegally, they come seeking a job. People use a Social Security card, often a fraudulent one, to get a job and this is the way to end that demand side, the magnet that draws them in, by having a structure in place like this. I agree that, overall, this is not the panacea, but I think that this will go an awful long way toward addressing this issue.

Chairman MCCRERY. Mr. Johnson?

Mr. JOHNSON. Thank you, Mr. Chairman. I am wondering how easy it is to duplicate a card like that.

Mr. DREIER. It is a great question, Sam, and I will tell you that one of the things that we have done is we have said that nothing has been done since 1935.

Mr. JOHNSON. Right.

Mr. DREIER. I believe that with the technological advances that are made, that it would be, I hope, impossible to duplicate it. There are no guarantees, but we should do every single thing within our power to, after these many decades having done nothing, use the technology that we have today to ensure that it is as tamper-proof, as smart, as counterfeit-proof as we possibly can.

Mr. JOHNSON. I couldn't agree with you more. What kind of upgrade are you going to have to have to get—business offices don't have the ability to scan cards, a lot of them.

Mr. DREIER. Well, that is a great question, and obviously this is something that would have to be phased in over a period of time. At the end of the day, I think that it would be easier on businesses because of the fact that they don't have to look at these 94 different combinations of documents, and I am, frankly, offended by a lot of this stuff where you would ask one person whether or not they are an American citizen and not another person based in the way someone might look. I am very offended by that. I think that the existence of this card will go a long way toward helping that. Obviously, we will have to deal with businesses as they look at the challenge of having the equipment—

Mr. JOHNSON. Yes, there is going to be a cost involved. You are from California, and you have got a lot of agricultural migrant workers out there. How are you going to get them a card?

Mr. DREIER. You know what? The fact—

Mr. JOHNSON. Are we going to—let me rephrase it a little bit.

Mr. DREIER. Sure.

Mr. JOHNSON. Guys that come across legally for migrant work, are we going to give them some kind of an identification?

Mr. DREIER. Well, see, what they would have on this is they would, within the database, it would be stated that they are here, if it is an H-2A visa or any kind of work permit, that would mean that they are a qualified worker by virtue of it. If we do end up with some kind of responsible non-amnesty-granting temporary worker program, someone who is here under that would be able to have this card for those purposes. If someone is here illegally and they don't have a card and they are hired, then that employer would be subjected to a, as I said, a 400-percent increase in the fine, 5 years in prison, and we hire 10,000 enforcement agents to make sure that this is enforced, which gets back to Silver's point, which is a very important one.

If you look at IRCA, we coupled amnesty with sanctions and un-enforced sanctions is what ended up once again reigniting this flow of people in illegally——

Mr. JOHNSON. Well, that is what I was about to say. If you depend on the employer, they are not going to do it.

Mr. DREIER. Exactly.

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. DREIER. I will say that I didn't believe that the employer should be turned into a Border Patrol agent.

Mr. JOHNSON. I agree.

Mr. DREIER. That is one of the concerns that I have, and I know we share that. I voted against the—I was here in 1986 and voted against IRCA for that reason.

Mr. JOHNSON. Thank you.

Chairman MCCRERY. Thank you, Mr. Johnson. Mr. Becerra?

Mr. BECERRA. Thank you to the two of you for being here and making your presentation. It is rather interesting. We are about to have witnesses who will come and give us testimony on the Social Security card, the use of the number, and so forth, and we have had over the course of actually the last few years a number of hearings. Last session, we passed out, without a single "no" vote, legislation by Representative Shaw to actually restrict the use of the SSN. It is interesting, because your proposal would make it the universal identifier and we are about to hear from witnesses who are going to tell us why there are problems in allowing the number to be more universally available. It is a fascinating discussion.

We need to figure out a way to be able to identify folks. Right now, the SSA would tell you, if they were here to testify, that just by having a number, we can't tell you, or they can't tell us if that individual is a citizen——

Mr. DREIER. Absolutely.

Mr. BECERRA. —or not. They may or may not be able to tell us whether that person is here legally. You would have to do a lot of work before you could get the SSN to become a national identification number.

Mr. DREIER. Well, we don't want it to be that, though. We don't want it to be a national ID card. In fact, as I said, we actually have on this card that it is not a national ID card and it is used only for Social Security purposes and when applying for a new job.

Mr. BECERRA. Okay, so then, Mr. Chairman, let me ask you this. What are you going to tell all the credit bureaus, the banks, all the folks, all the industries that currently use the SSN—hospitals used to use them publicly as the patient identification number—what do you tell all those industries that are telling us right now, you can't do more to restrict our utilization of the number because that has become our universal identifier within our industry?

Mr. DREIER. You see, that is up to them. What I have said is a national ID card, getting on board an airplane, utilizing it for a Federal purpose, which is really what we are in the business of doing. The way some private entity or a State or local entity handles the use of this number and card is their business——

Mr. BECERRA. Would you prohibit the use for any other purposes?

Mr. DREIER. Yes, I am not saying—I am not saying that it can't be used, because I don't want to in any way restrict the SSN from being utilized for purposes that we determine are necessary. All I am saying is that I don't want the use of a smart, counterfeit-proof Social Security card to be misinterpreted as some sort of national identification card. That is all I am arguing.

Mr. BECERRA. The thing there, David, is if indeed it is a strong identifier that has good firewalls from abuse, then it is going to become a great identifier for a lot of other folks, as well. If it works well for identifying whether or not you are entitled to work in this country, someone is going to say, well, it is probably going to work well to identify whether or not you have got good credit or whether or not we should offer you this mortgage. I think we have to be very careful. Unless you prohibit its use for other purposes—

Mr. DREIER. I think that is something we might consider looking at, if you want to.

Mr. REYES. If I can say something, currently—I just became a grandfather for the third time. When your baby is born, he or she gets a Social Security card.

Mr. BECERRA. Yes.

Mr. REYES. When you volunteer for the Army or the Navy, the Marine Corps, the Air Force, your Social Security card becomes your identifier. When I was drafted, I was given a number, RN-18746717. You never forget that. Today's service people use that Social Security card for those purposes. I don't know that—and maybe David has given it more thought, but I haven't given it a lot of thought in terms of why you would want to preclude or limit somebody's ability to use the SSN when I know—

Mr. BECERRA. If you were to stay a little longer, you would hear testimony by someone who actually had her SSN misused for identity purposes—

Mr. REYES. See, even in this system, I think here is what is important about having the system. I made the three points. The system would tell you if somebody else is using the same number, because in today's technology, the availability—if somebody presents—say, for instance, somebody came up with a system of—

Mr. BECERRA. Yes, but by then, it is too late—

Mr. REYES. No—

Mr. BECERRA. —for the person who had his or her identity stolen.

Mr. REYES. The point is, it will raise an alert when that card is presented. It is like—and I don't know how they work currently on use of credit cards, but I know that occasionally when I give a credit card, especially when you travel out of the country, they will ask for identification. My wife will get a call at home and say, this purchase was made in London or whatever. We want to make sure that you or your husband is comfortable that one of you is in London.

The technology exists that would be able to tell the system that the SSN that was presented in Peoria, Illinois, all of a sudden a week later was presented in Los Angeles and maybe within 72 hours was presented within Miami, so that tells you that number has been compromised somehow and the system alerts DHS and they would check all three people that presented that card.

Mr. DREIER. Which one of the two of you is making all those purchases, too.

Mr. REYES. Yes.

Mr. BECERRA. Thank you, Mr. Chairman. Thank you, gentlemen.

Chairman MCCRERY. Mr. Brady?

Mr. BRADY. Thank you, Mr. Chairman, and David and Grandpa Reyes, it is good to have you here today. I think Xavier's comment about SSNs, one of the issues we are struggling with is our SSN system already so compromised that we can never really bring integrity to the system. Your point is that if Social Security is going to be a key employer verification in this whole immigration-Border Security debate, make it counterfeit-proof. Here is the way to do it.

I think, in the end, the question of whether we will have a counterfeit or attempt to create a counterfeit Social Security document, it isn't a matter of if we do but when and how we do it, how we structure it, and I know that I supported the House bill on border security that passed earlier, or late last year, but I know that today, if we had to rely on the Social Security system to verify workers in this country, either new or existing, the system would simply crater. It doesn't have the integrity, the resources, the technology to do that, so I just appreciate you bringing a bipartisan idea to the table and I appreciate you, Chairman, letting us hear what some of our Members who are giving this issue some thought a chance to talk to us about that.

I don't really have any questions. Thanks for giving this a thoughtful—

Mr. DREIER. Let me just thank you very much for that, Kevin, and say that I believe that we are in a position where this can go a long way toward addressing those identity issues, which Xavier correctly raised, dealing with the question that Sandy raised as to exactly what happens to the people who are here, and tackles this whole issue of the credibility of Social Security and the utilization of the number itself as we head to the future.

I had a conversation yesterday with a number of Senators about this. They are in the midst of their debate on this, and I should say that this provision is actually included in one of the Senate bills that has been introduced. John Cornyn and Jon Kyl have introduced legislation that actually includes H.R. 98 as an important component of it.

It is my hope that we will be able to see this move as expeditiously as possible through so that we can include this as part of a comprehensive package, and I certainly leave it up to you all to demonstrate for us what the best approach is.

Chairman MCCRERY. Thank you, Mr. Brady.

Mr. Dreier, Mr. Reyes, thank you very much for being with us—

Mr. DREIER. Thank you very much for having us.

Chairman MCCRERY. —and for showing up today and sharing with us your thoughts.

Mr. DREIER. Thanks, Mr. Chairman.

Chairman MCCRERY. Our next panel is composed of two witnesses, Ms. Cynthia Fagnoni, Managing Director of Education, Work force, and Income Security, United States GAO, and Joel

Winston, the Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission.

Your written testimony will be included in the record in its entirety and we would like for you to try to summarize your written testimony in about 5 minutes, and Ms. Fagnoni, we will begin with you. Welcome.

**STATEMENT OF CYNTHIA M. FAGNONI, MANAGING DIRECTOR,
EDUCATION, WORKFORCE, AND INCOME SECURITY ISSUES,
U.S. GOVERNMENT ACCOUNTABILITY OFFICE**

Ms. FAGNONI. Thank you. Thank you, Mr. Chairman, Mr. Levin, and Members of the Subcommittee. I am pleased to be here this afternoon to discuss ways to better protect the SSN.

Although the SSN was originally created as a means of tracking workers' earnings and eligibility for Social Security benefits, today, the number is used for many non-Social Security purposes. The wide use of the SSN is significant because once it is obtained fraudulently, it can be used to create false identities for financial misuse, to falsely obtain credit, or to assume another person's identity.

Today, I would like to discuss the use of SSNs by government agencies and certain private sector entities, Federal laws that regulate the use and disclosure of SSNs, and gaps that remain in protecting the SSN and what more could be done. My testimony is based on reports GAO has issued over the last several years, many of them completed at the request of this Subcommittee.

First, let me begin with the widespread use of SSNs by both the public and private sectors. Federal, State, and county government agencies rely extensively on the SSN to maintain records with unique identifiers and ensure program integrity. Last year, we reported that SSNs are available in a variety of public records held by States, local jurisdictions, and courts, public records or documents routinely made available to the public for inspection, such as marriage licenses and property transactions. We also reported that information resellers, consumer reporting agencies, and health care organizations use SSNs for a variety of purposes, including verifying a person's identity or matching existing records.

Earlier this year, we reported that banks, security firms, telecommunications companies, and tax preparation companies routinely obtain SSNs from their customers for authentication and verification purposes and sometimes share SSNs with their contractors for limited purposes, such as identification requirements, debt collection, and data storage.

Regarding the laws, although Federal and State laws have been enacted to restrict the use and disclosure of consumers' personal information, including SSNs, no one law comprehensively regulates the SSN use and protections. Moreover, many of the laws enacted are industry-specific and do not apply broadly.

Several States have enacted laws to restrict the use and display of SSNs. California, for example, has enacted such a law. Thirteen other States now have passed laws similar to California's. Four States—California, Georgia, Nevada, and New York—require notification of security breaches, another example. As a result of such

State restrictions, some companies now notify customers of security breaches regardless of where they happen in the country.

Although Congress and State legislatures have enacted laws that help to restrict SSN display and protect an individual's personal information, we have found gaps in the protection of SSNs. We have reported that government agencies at all levels lack the uniform approach to ensuring the security of the SSN. In addition, we found that gaps exist in the Federal law and oversight of different industries that share SSNs with their contractors. SSNs also continue to be exposed on government-issued ID cards. Finally, few restrictions are placed on information resellers to obtain and resell SSNs in the course of their business.

GAO has made a number of recommendations in proposed matters for Congressional consideration to address these gaps. We propose that Congress pull together a representative group of Federal, State, and local officials to develop a unified approach to safeguarding SSNs used at all levels of government. We also recommended that OMB advise all levels of government of the applicability of the Privacy Act (P.L. 93-579) and develop a government-wide policy to ensure a consistent approach for displaying SSNs on ID cards.

Regarding the private sector, we have recommended that Congress consider possible options for addressing the gaps in the existing Federal requirements for safeguarding SSNs shared with contractors. We continue to focus on SSN issues, identify gaps, and will continue to recommend possible solutions, where appropriate.

Mr. Chairman, this completes my oral statement. I would be happy to answer any questions you or other Members of the Subcommittee may have. Thank you.

[The prepared statement of Ms. Fagnoni follows:]

Statement of Cynthia M. Fagnoni, Managing Director, Education, Workforce, and Income Security, U.S. Government Accountability Office

Mr. Chairman and Members of the Committees:

I am pleased to be here today to discuss ways to better protect the Social Security Number (SSN). The SSN was created as a means to track workers' earnings and eligibility for Social Security benefits. However, the SSN has evolved beyond its original intended purpose and has become the identifier of choice for public and private sector entities, and is used for numerous non-Social Security purposes. This is significant because SSNs, along with a name and date of birth, are the pieces of information most often sought by identity thieves. Once an SSN is obtained fraudulently, it can then be used to create false identities for financial misuse, assuming another individual's identity, fraudulently obtaining credit, violating immigration laws, or fleeing the criminal justice system. Recent statistics suggest that the incidence of identity theft is rapidly growing. The Federal Trade Commission (FTC) estimated that over a 1-year period nearly 10 million people—or 4.6 percent of the adult U.S. population—discovered that they were victims of some form of identity theft, translating into estimated losses exceeding \$50 billion. FTC also reported that most victims of identity theft do not report the crime, and, therefore, the total number of identity theft incidences is unknown.

Over the last few years Congress and some states have recognized the importance of restricting the use and display of SSNs by both public and private sectors. As a result, federal and state laws have begun to be enacted that to some degree protect individual's personal information, including SSNs. GAO has issued a number of reports and testified before this Subcommittee about the various aspects of SSN use in both the public and private sectors. (See related GAO products at the end of this testimony.) Accordingly, you asked us to speak about some of our findings regarding SSN use and protections. My remarks today will focus on (1) the use of SSNs by government agencies and certain private sector entities, (2) the federal

laws that regulate the use and disclosure of SSNs, and (3) the gaps that remain in protecting the SSN and what more could be done.

In summary, SSN use is widespread by both the public and private sectors. Agencies at all levels of government frequently collect and use SSNs to administer their programs, verify applicants' eligibility for services and benefits, and perform research and evaluations of their programs. In addition, SSNs are available in a variety of public records held by states, local jurisdictions, and courts, appearing in records that document common life events and transactions, such as marriages and home purchases. Certain private sector entities also use SSNs. Information resellers, credit reporting agencies (CRAs), and health care organizations routinely obtain SSNs from various public and private sources, and use SSNs for various purposes, such as to build tools that verify an individual's identity or match existing records. In addition, private sector entities that engage in third party contracting sometimes share SSNs with their contractors for limited purposes.

There is no one law that comprehensively regulates SSN use and protections. However, certain federal laws have been enacted to restrict the use and disclosure of consumers' personal information, including SSNs, but these laws tend to be industry-specific and do not apply broadly. In addition, certain states had begun to enact their own legislation restricting the use and display of SSNs by public and private sector entities, which has subsequently led other states to start enacting similar regulation. Finally, Congress is currently considering several proposals to restrict SSN use and display, similar to state legislation.

Although some action has been taken at the federal and state level to protect SSNs, more could be done. In our prior work, we found gaps in the practices for protecting SSNs by government agencies and across industry sectors. As a result, we made recommendations to federal agencies to address the issues we found and proposed matters for Congress to consider. For example, we found that certain measures that could help protect SSNs are not uniformly in place at all levels of government. In addition, there are gaps in the federal law and oversight in different industries that share SSNs with their contractors, and there are few restrictions placed on certain entities' abilities to obtain and use SSNs in the course of their business. Finally, SSNs are widely exposed in a variety of public records and are still subject to exposure on identity cards issued under federal auspices. To address some of these issues, we made recommendations and proposed matters for congressional consideration. For example, to address gaps in the government uses of SSNs and the exposure of SSNs in public records and on identification cards, we advised Congress to convene a group of government officials to develop a unified approach to safeguarding SSNs. To address the gaps in federal laws that would apply to industries that share SSNs with their contractors, we recommended Congress consider options to restrict the use and display of SSNs to third party contractors.

Background

The Social Security Act of 1935 authorized the Social Security Administration (SSA) to establish a record-keeping system to manage the Social Security program, which resulted in the creation of the SSN.¹ Through a process known as "enumeration," unique numbers are created for every person as a work and retirement benefit record. Today, SSA issues SSNs to most U.S. citizens, but they are also available to non-citizens lawfully admitted to the United States with permission to work. Lawfully admitted noncitizens may also qualify for a SSN for nonwork purposes when a federal, state, or local law requires that they have a SSN to obtain a particular welfare benefit or service. SSA staff collect and verify information from such applicants regarding their age, identity, citizenship, and immigration status.

With the enhancement of computer technologies in recent years, private sector businesses are increasingly computerizing their records; as a result, these enhancements have spawned new businesses activities involving the aggregation of person information. Information resellers, sometimes referred to as information brokers, are businesses that specialize in amassing consumer information including SSNs for informational services. They may provide their services to a variety of customers, either to specific businesses clients or through the Internet to anyone willing to pay a fee. Consumer reporting agencies, also known as credit bureaus, are agencies that collect and sell information about the creditworthiness of individuals. CRAs collect information that is considered relevant to a person's credit history, and obtain SSNs from their customers or businesses that furnish data to them, as well as from private and public sources. Organizations that provide health care services also com-

¹ The Social Security Act of 1935 created the Social Security Board, which was renamed the Social Security Administration in 1946.

monly use consumers' SSNs. They obtain SSNs from individuals themselves and companies that offer health care plans.

In recent years, companies have increasingly relied on the use of contractors to perform certain activities and functions related to their business operations. This trend has often been referred to as outsourcing. However, no commonly recognized definition of outsourcing exists, and there has been confusion over whether it encompasses only activities a company performed in-house or includes any activity a company may contract out. According to outsourcing experts, approximately 90 percent of businesses contract out some activity because they find either it is more economical to do so or other companies are better able to perform these activities. Some of the activities companies outsource will require that contractors be provided personal information about the companies' customers in order to perform those activities, in some cases, this information includes SSNs.

Due to the pervasive use of SSNs, individuals are routinely asked to disclose their SSNs, along with other personal identifying information, for numerous purposes. In some instances where individuals provide their SSNs to government entities, documents containing the SSN are routinely made available to the public for inspection. The widespread disclosure of SSNs in public records has raised concern because it can put individuals at increased risk of identity theft. In addition, given the explosion in the Internet use and the ease with which personally identifiable information is accessible, individuals looking to steal someone's identity are increasingly able to do so. According to FTC, it receives roughly 15,000 to 20,000 contacts per week on its hotline and Web site, or through the mail from victims and consumers who want to avoid becoming victims.

Both Government and Private Sector Entities Collect and Use SSNs for a Variety of Purposes

Government entities are generally required by law to collect SSNs to determine individuals' eligibility for services and benefits. SSNs are also widely available in public records maintained by state and local governments and the courts. Certain private sector entities, such as information resellers, CRAs, and healthcare organizations obtain SSNs from public and private sources, or directly from their customers, and use them for various purposes. In addition, banks, securities firms, telecommunication firms, and tax preparers engage in third party contracting and sometimes share SSNs with their contractors for limited purposes.

Government Entities Are Required by Laws and Regulations to Collect SSNs, and Use Them for Various Purposes

As required by a number of federal laws and regulations, agencies at all levels of government frequently collect and use SSNs to administer their programs, to link data for verifying applicants' eligibility for services and benefits, and to conduct program evaluations.² For example, the Personal Responsibility and Work Opportunity Act of 1996 mandates that, among other things, states have laws in place to require the collection of SSNs on driver's license applications. Such laws and regulations have contributed to the widespread use of SSNs by government agencies, because the SSN serves as a unique identifier.

Government agencies use SSNs for a variety of purposes. We have found that agencies typically used SSNs to manage their records and to facilitate data sharing to verify an applicant's eligibility for services and benefits.³ For example, agencies use SSNs

- for internal administrative purposes, which included activities such as identifying, retrieving, and updating records;
- to collect debts owed the government and conduct or support research and evaluations as well as using employees' SSNs for activities such as payroll, wage reporting, and providing employee benefits;
- to ensure program integrity, such as matching records with state and local correctional facilities to identify individuals for whom the agency should terminate benefit payments; and
- for statistics, research, and evaluation;⁴

²GAO, Social Security: Government and Commercial Use of the Social Security Number Is Widespread, GAO/HEHS-99-28 (Washington, D.C.: February 16, 1999) and GAO, Social Security Numbers: Government Benefits from SSN Use, but Could Provide Better Safeguards, GA0-02-352 (Washington, D.C.: May 31, 2002).

³GAO-02-352.

⁴The Bureau of the Census is authorized by statute to collect a variety of information and is prohibited from making it available, except in certain circumstances.

SSNs Are Widely Available in Public Records Held by States, Local Jurisdictions, and Courts, but Many of These Agencies Are Taking Steps to Limit Display

SSNs are publicly available throughout the United States, primarily at the state and local levels of government.⁵ Based on a survey of federal, state, and local governments, we reported in 2004 that state agencies in 41 states and the District of Columbia were displaying SSNs in public records; this was also true in 75 percent of U.S. counties.⁶ We also found that while the number and type of records in which SSNs were displayed varied greatly across states and counties, SSNs were most often found in court and property records.

Public records displaying SSNs are stored in multiple formats that vary by different levels of government. State government offices tended to store such records electronically, while most local government records were stored on microfiche or microfilm. However, our survey found that public access to such records was often limited to inspection of the individual paper copy or request by mail.⁷

We found that few state agencies make public records available on the Internet, although some do so. However, few state or local offices reported any plans to significantly expand Internet access to public records that display SSNs. Based on our survey results, only four state agencies indicated plans to make such records available on the Internet, and one agency planned to remove records displaying SSNs from Internet access.

Private Sector Entities Obtain SSNs from Public and Private Sources and Use Them for Various Purposes

Private sector entities such as information resellers, CRAs, and health care organizations generally obtain SSNs from various public and private sources. Large or well known information resellers have told us they obtain SSNs from various public records, such as records of bankruptcies, tax liens, civil judgments, criminal histories, deaths, real estate transactions, voter registrations, and professional licenses. They also said that they sometimes obtain batch files of electronic copies of jurisdictional public records where available. However, some reseller officials said they are more likely to rely on SSNs obtained directly from their clients, who would voluntarily provide such information for a specific service or product, than those found in public records.⁸

Like information resellers, CRAs also obtain SSNs from public and private sources. CRA officials have told us that they obtained SSNs from public sources, such as bankruptcy records. We also found that these companies obtained SSNs from other information resellers, especially those that specialized in obtaining information from public records. However, CRAs are more likely to obtain SSNs from businesses that subscribe to their services, such as banks, insurance companies, mortgage companies, debt collection agencies, child support enforcement agencies, credit grantors, and employment screening companies. Therefore, individuals who provide these businesses with their SSNs for reasons such as applying for credit would subsequently have their charges and payment transactions, accompanied by the SSN, reported to the CRAs.

Health care organizations, including health care insurance plans and providers, are less likely to obtain SSN data from public sources. Health care organizations typically obtained SSNs either from individuals themselves or from companies that offer health care plans. For example, subscribers or policyholders enrolled in a health care plan provide their SSN as part of their health care plan application to their company or employer group. In addition to health care plans, health care organizations also included health care providers, such as hospitals. Such entities often collected SSNs as part of the process of obtaining information on insured people. However, health care provider officials told us that, particularly with hospitals, the medical record number is the primary identifier, rather than the SSN.

⁵ Not all records held by government or public agents are "public" in terms of their availability to any inquiring person. For example, adoption records are generally sealed. Personnel records are often not readily available to the public, although newspapers may publish the salaries of high, elected officials. There is no common definition of public records. However, we define public records as those records generally made available to the public for inspection in their entirety by a federal, state, or local government agency. Such documents are typically accessed in a public reading room, clerk's office, or on the Internet.

⁶ GAO, Social Security Numbers: Governments Could Do More To Reduce Display in Public Records and on Identity Cards, GAO-05-59 (Washington, D.C.: November 9, 2004).

⁷ GAO-05-59

⁸ GAO, Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information, GAO-04-11 (Washington, D.C.: January 22, 2004).

We found that the primary use of the SSN by information resellers, CRAs, and health care organizations alike was to help verify the identity of an individual. Large information resellers said they generally use the SSN as an identity verification tool. They also use it for internal matching purposes of its databases, as a factor in identifying individuals for their product reports, or for conducting investigations for their clients for resident screening or employment screening. CRAs use SSNs as the primary identifier of individuals that enables them to match the information they receive from their business clients with information stored in their databases on individuals. Because these companies have various commercial, financial, and government agencies furnishing data to them, the SSN is the primary factor that ensures that incoming data is matched correctly with an individual's information on file. We found that in some cases CRAs and information resellers can sometimes be the same entity, a fact that blurs the distinction between the two types of businesses but does not affect the use of SSNs by these entities. Finally, health care organizations also use the SSN to help verify the identity of individuals. These organizations use SSNs, along with other information such as name, address, and date of birth, as a factor in determining a member's identity.

Private sector companies also share customers' SSNs with their contractors. Banks, investment firms, telecommunication companies, and tax preparation companies we interviewed routinely obtain SSNs from their customers for authentication and identification purposes.⁹ All these companies contracted out various services, such as data processing, administrative, and customer service functions. Although these companies may share consumer information, such as SSNs, with contractors that provide services to their customers, company officials said that they only share such information with their contractors for limited purposes, generally when it is necessary or unavoidable.

The companies we contacted provided us with standard contract forms they use in contracting with service providers to safeguard customers' personal information, such as SSNs, from misuse.¹⁰ In general, the types of provisions these companies included in their standard contract forms included electronic and physical data protections, audit rights, data breach notifications, subcontractor restrictions, and data handling and disposal requirements. We found that most of the companies we interviewed had established some type of due diligence or credentialing process to verify the reliability of potential contractors prior to and during contract negotiations. Furthermore, we found that some industry associations have voluntarily developed guidance for their members regarding the sharing of personal information with third parties.

No Single Law Governs the Use and Disclosure of SSNs Although Various Laws Have Been Enacted That Help Protect SSNs

Although no single law comprehensively governs the use and disclosure of SSNs, certain federal laws restrict the use and disclosure of personal information, including SSNs, by government agencies or private sector entities. These laws, however, tend to be directed at specific industries or governmental agencies and often do not apply broadly across public and private sectors or across private sector industries. For example, the overall use and disclosure of SSNs by the federal government is restricted under the Privacy Act, which, broadly speaking, seeks to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy. The Privacy Act requires that any federal, state, or local government agency, when requesting an SSN from an individual, tell individuals whether disclosing their SSN is mandatory or voluntary, cite the statutory or other authority under which the request is being made, and state what uses it will make of the individual's SSN.

Other federal laws have also placed restrictions on private sector entities' use and disclosure of consumers' personal information, including SSNs. These include the Fair Credit Reporting Act (FCRA), the Fair and Accurate Credit Transaction Act (FACTA), the Gramm-Leach-Bliley Act (GLBA), the Drivers Privacy Protection Act (DPPA), and the Health Insurance Portability and Accountability Act (HIPAA). As shown in table 1, some of these federal laws either restrict certain private sector entities from disclosing personally identifiable information to specific purposes or with whom the information is shared. In addition, certain industries, such as the financial services industry, are required to protect individuals' personal information to a greater degree than entities in other industries.

⁹ GAO, Social Security Numbers: Stronger Protections Needed When Contractors Have Access to SSNs, GAO-06-238 (Washington, D.C.: January 23, 2006).

¹⁰ GAO-06-238

Table 1: Aspects of Federal Laws That Affect Private Sector Disclosure of Personal Information

Federal Laws	Restrictions
Fair Credit Reporting Act	Limits access to credit data that includes SSNs to those who have a permissible purpose under the law.
Fair and Accurate Credit Transactions Act	Amends FCRA to allow, among others things, consumers who request a copy of their credit report to also request that the first 5 digits of their SSN (or similar identification number) not be included in the file; requires consumer reporting agencies and any business that use a consumer report to adopt procedures for proper disposal.
Gramm-Leach-Bliley Act	Creates a new definition of personal information that includes SSNs and limits when financial institutions may disclose the information to nonaffiliated third parties.
Health Insurance Portability and Accountability Act	Protects the privacy of health information that identifies an individual and restricts health care organizations from disclosing such information to others without the patient's consent.

Source: GAO analysis

Congress has also introduced a federal statute that criminalizes fraud in connection with the unlawful theft and misuse of personal identifiable information. In 1998, Congress enacted the Identity Theft and Assumption Deterrence Act (Identity Theft Act). The act made it a criminal offense for a person to “knowingly transfer, possess, or use without lawful authority,” another person’s means of identification “with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law.” Under the act, a name or Social Security number is considered a “means of identification” and a number of cases have been prosecuted under this law.

Many states have begun to enact laws to restrict the use and display of SSNs. (See appendix 1 for a listing of state laws previously reported by GAO.) After one state took action, other states followed in enacting similar laws. For example, in 2001, California enacted a law restricting the use and display of SSNs, which generally prohibited companies and persons from engaging in certain activities, such as posting or publicly displaying SSNs, or requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted. In addition, California enacted a law containing notification requirements in the event of a security breach where a business or a California state agency is required to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Subsequently, other states have enacted laws restricting the use and display of SSNs. Specifically, in our prior work, we identified 13 others states—Arizona, Arkansas, Connecticut, Georgia, Illinois, Maryland, Michigan, Minnesota, Missouri, Oklahoma, Texas, Utah, and Virginia—that have each passed laws similar to California’s.¹¹ While some states, such as Arizona, have enacted virtually identical SSN use and display restrictions, other states have modified the restrictions in various ways. For example, unlike the California law, which prohibits the use of the full SSN, the Michigan statute prohibits the use of more than four sequential digits of the SSN. The Michigan law also contains a prohibition against the use of SSNs on identification and membership cards, permits, and licenses. Missouri’s law includes a prohibition against requiring an individual to use his or her SSN as an employee number. Oklahoma’s law is unique in that it only limits the ways in which employ-

¹¹ See Arkansas (Ark. Code Ann. § 4-86-107 (2005)); Arizona (Ariz. Rev. Stat. § 44-1373 (2004)); Connecticut (Conn. Gen. Stat. § 42-470 (2003)); Georgia (Ga. Code Ann. § 33-24-57.1 (2003)); Illinois (815 Ill. Comp. Stat. 505/2QQ (2004)); Maryland (Md. Code Ann., Com. Law § 14-3301 et seq. (2005)); Michigan (Mich. Comp. Laws § 445.81 et seq. (2004)); Minnesota (Minn. Stat. § 325E.59 (2005)); Missouri (Mo. Rev. Stat. § 407.1355 (2003)); Oklahoma (Okla. Stat. tit. 40, § 173.1 (2004)); Texas (Tex. Bus. & Com. Code Ann. 35.58 (2003)); Utah (Utah Code Ann. § 31A-21-110 (2004)); and Virginia (Va. Code Ann. § 59.1-443.2 (2005)).

ers may use their employees' SSNs, and does not apply more generally to other types of transactions and activities.

Some states have recently enacted other types of restrictions on the uses of SSNs as well. Arkansas, Colorado, and Wisconsin limit the use of a student's SSN as a student identification number.¹² New Mexico requires businesses that have acquired consumer SSNs to adopt internal policies to limit access to authorized employees.¹³ Texas recently enacted a law requiring businesses to properly dispose of business records that contain a customer's personal identifying information, which is defined to include SSNs.¹⁴

Other recent state legislation includes new restrictions on state and local government agencies. For example, South Dakota law prohibits the display of SSNs on all driver's licenses and nondriver's identification cards,¹⁵ while Indiana law generally prohibits a state agency from releasing a SSN unless otherwise required by law.¹⁶ In addition, as of January 1, 2007, a Nevada law will require governmental agencies, except in certain circumstances, to ensure that the SSNs recorded in their books and on their records are maintained in a confidential manner.¹⁷

We also identified four states that have passed legislation containing notification requirements in the event of a security breach. For example, New York recently enacted a law requiring such notifications.¹⁸ California requires a business or a California state agency to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.¹⁹ In the last year, this law forced several large companies to notify individuals that their information was compromised because of certain circumstances. Under a Nevada law, government agencies and certain persons who do business in the state must notify individuals if their personal information is reasonably believed to have been compromised.²⁰ Similarly, Georgia requires certain private sector entities to notify their customers if a security breach occurred that compromised their customers' personal information, such as their SSNs.²¹

In addition, we found that some state offices were beginning to take measures to change the way in which they displayed or shared SSNs in public records. For example, we found that many state agencies had restricted access to or redacted—covered or otherwise hidden from view—SSNs from public versions of records. Specific restrictions and other actions state agencies reported taking included blocking or removing SSNs from electronic versions of records, allowing individuals identified in the record to request removing their SSN from the publicly available version, replacing SSNs with alternative identifiers, and restricting access only to individuals identified in the records.

Finally, Congress is currently considering consumer privacy legislation, which in some cases includes SSN restrictions. In 2005, there were more than 20 proposed bills pending before the U.S. House and Senate.²² In some cases, the provisions being considered mirrored provisions in enacted state laws. For example, some proposed legislation included prohibitions on the display of SSNs, similar to a Colorado law, while other proposed legislation address the solicitation of SSNs by public and private sector entities. In addition, some federal privacy legislation also proposed consumer safeguards, such as security freezes and prohibitions on the sale and purchase of SSNs.

More Could Be Done To Protect SSNs

Although laws at both state and federal levels have helped to restrict SSN display and protect individual's personal information, clearly gaps remain. We have issued a number of reports for this Subcommittee that have looked at the collection, use, and protections of SSNs by federal agencies and private sector entities. In some cases where federal action could be taken, we have proposed matters for congressional consideration to explore legislative actions or recommendations to a federal agency to address problems we found. In other cases, mainly those that relate to

¹² Ark. Code Ann. § 6-18-208 (2005); Colo. Rev. Stat. § 23-5-127 (2003); and Wis. Stat. § 36.32 (2001).

¹³ N.M. Stat. Ann. § 57-12B-1 et seq. (2003).

¹⁴ Tex. Bus. & Com. Code Ann. § 35.48 (2005).

¹⁵ S.D. Codified Laws § 32-12-17.13 (2005).

¹⁶ Ind. Code § 4-1-10-1 et seq. (2005).

¹⁷ Nev. Rev. Stat. § 239.030 (2005).

¹⁸ N.Y. State Tech. Law § 208 (2005).

¹⁹ Cal. Civ. Code § 1798.29 (2002); 1798.82 (2002).

²⁰ Nev. Rev. Stat. § 603A.220 (2005).

²¹ Ga. Code Ann. § 10-1-910 et seq. (2005).

²² GAO, Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain, GAO-05-1016T (Washington, D.C.: September 15, 2005)

private sector entities, we have proposed a matter for Congressional consideration. OMB has implemented two of our recommendations and Congress is still considering what actions need to be taken.

Prior Work Found Gaps in the Protections of SSNs

In our review of government uses of SSNs, we reported that certain measures that could provide more assurances that SSNs obtained by government entities are secure are not universally in place at any level of government.²³ Agencies that deliver services and benefits use SSNs to administer programs and took some steps to safeguard SSNs. However, when federal, state, and county agencies request SSNs, they did not consistently inform the SSN holders of whether they must provide the SSN to receive benefits or services and how the SSN will be used. In addition, although some agencies took action to limit the display of SSNs on documents that were not intended to be public but may be viewed by others, these actions sometimes took place in a piecemeal manner rather than as a result of a systematic effort.

In our reviews of private sector entities' collection and use of SSNs, we found gaps in how different industries are covered by federal laws protecting individual's personal information. In our third party contractors' review, we reported that federal regulation and oversight of SSN sharing varies across four industries we reviewed, revealing gaps in federal law and agency oversight for different industries that share SSNs with their contractors.²⁴ For example, federal law and oversight of the sharing of personal information in the financial services industry is very extensive: financial services companies must comply with GLBA requirements for safeguarding customer's personal information, and regulators have an examination process in place that includes determining whether banks and securities firms are safeguarding this information. IRS has regulations and guidance in place to restrict the disclosure of SSNs by tax preparers and their contractors, but does not perform periodic reviews of tax preparers' compliance. FCC does not have regulations covering SSNs and also does not periodically review telecommunications companies to determine whether they are safeguarding such information. Companies in the industries we reviewed relied on accepted industry practices and primarily used the terms of their contracts to safeguard personal information, including SSNs they shared with outside contractors.

We also found that there are few restrictions placed on certain entities' abilities such as information resellers to resell SSNs in the course of their business. Although certain federal laws have some restrictions on reselling nonpublic personal information, these laws only apply to certain types of private sector entities, such as financial institutions.

In our review of SSNs in public records, we found that SSNs are widely exposed to view in a variety of public records and are still subject to exposure on identity cards issued under federal auspices.²⁵ The number and type of records in which SSNs are displayed varies greatly for both states and counties, and SSNs are available in some federal court records. A number of government agencies and oversight bodies are taking steps to eliminate the open display of SSNs. For example, some actions state agencies reported taking included blocking or removing SSNs from electronic versions of records, and replacing SSNs with alternative identifiers. However, such initiatives to protect the SSN may slow its misuse, but the absence of uniform and comprehensive policy is likely to leave many individuals vulnerable.

Finally, although they are not displayed in public records en masse, we found that millions of SSNs are still subject to exposure on individual identity cards issued under federal auspices. We found that in 2004 an estimated 42 million Medicare cards displayed entire 9-digit SSNs, as did approximately 8 million Department of Defense (DOD) insurance cards and 7 million Department of Veterans Affairs (VA) beneficiary cards. Some of these agencies have begun taking action to remove SSNs from identification cards. For example, VA is eliminating SSNs from 7 million VA identification cards and is replacing cards with SSNs or issuing new cards without SSNs from 2004 through 2009, until all such cards have been replaced. DOD has begun replacing approximately 6 million health insurance cards that display SSNs with cards that do not display the bearer's SSN, but continues to include SSNs on approximately 8 million military identification cards. The Centers for Medicare and Medicaid Services, with the largest number of cards displaying the entire 9-digit SSN, does not plan to remove the SSN from Medicare identification cards.

²³ GAO-02-352

²⁴ GAO-06-238.

²⁵ GAO-05-59.

GAO Has Proposed Matters for Congressional Consideration and Recommendations

In order to address the issues we found, GAO has proposed matters for congressional consideration and recommended that a federal agency take action. To date, OMB has implemented two of our three recommendations, but Congress is still considering what other actions to take.

- In order to address the problems we found with how government entities assure the security of SSNs, we proposed that Congress consider convening a representative group of federal, state, and local officials to develop a unified approach to safeguarding SSNs used in all levels of government. The Privacy Act and other federal laws prescribe actions federal departments and agencies must take to assure the security of SSNs and other personal information. However, these requirements may not be uniformly observed. We presented a matter for congressional consideration to facilitate intergovernmental collaboration in strengthening safeguards at the state and local levels. We also made two recommendations to the Office of Management and Budget that it direct federal agencies to review their practices for securing SSNs and providing required information, and advise all federal, state, and local governments of the applicability of the Privacy Act to their uses of SSNs. OMB has implemented both our recommendations.
- In our report on third party contactors' uses of SSNs, we recommended that Congress consider possible options for addressing the gaps in existing federal requirements for safeguarding SSNs shared with contractors. The current gaps do not provide incentives for companies to commit to protecting personal information. Each industry is subject to different federal oversight and is often left to decide what established practices for safeguarding SSNs and other consumer information it wishes to follow. We suggested that one approach Congress could take would be to require industry-specific protections for the sharing of SSNs with contractors where such measures are not already in place. For example, Congress could consider whether the Telecommunications Act of 1996 should be amended to address how that industry shares SSNs with contractors. Alternatively, we suggested that Congress could take a broader approach. For example, in considering proposed legislation that would generally restrict the use and display of SSNs, Congress could also include a provision that would explicitly apply this restriction to third party contractors. We stated that with either approach, Congress would want to establish a mechanism overseeing compliance by contractors and enforcement.
- In our report on the display of SSNs on identification cards and in public records, we recommended that OMB identify all those federal activities that require or engage in the display of 9-digit SSNs on health insurance, identification, or any other cards issued to federal government personnel or program beneficiaries, and devise a governmentwide policy to ensure a consistent approach to this type of display. Although SSA has authority to issue policies and procedures over the Social Security cards that it issues, it does not have authority over how other federal agencies use and display SSNs. Rather, it is up to individual government agencies to have their own policies for the cards issued under their authority. The lack of a broad, uniform policy allows for inconsistent, but persistent exposure of the SSN. OMB has not yet taken action on our recommendation but said at the time we issued our report they would consider it. With regard to SSN exposure in public records, we again noted that it would be constructive for a representative group of federal, state, and local officials to develop a unified approach to safeguarding SSNs used in all levels of government, particularly those displayed in public records.
- Finally, with regard to private sector entities, such as information resellers reselling personal information, including SSNs, we noted that there are few restrictions placed on these entities ability to obtain, use, and resell SSNs for their businesses. The federal laws that have some restrictions can be interpreted broadly. The broad interpretation combined with the uncertainty about the application of the exceptions suggest that reselling personal information—including SSNs—is likely to continue.

Conclusions

The use of SSNs by both public and private sector entities is likely to continue given that it is used as the key identifier by most of these entities and there is currently no other widely accepted alternative. Given the significance of the SSN in committing fraud or stealing a person's identity, it is imperative that steps be taken

to protect it. Without proper safeguards in place, SSNs will remain vulnerable to misuse, thus adding to the growing number of identity theft victims.

SSNs are still widely used and publicly available, although becoming less so. State legislatures have begun to place restrictions on SSNs by enacting laws that restrict the use and display of SSNs and prohibit the theft of individuals' personal information. Yet, more could be done to protect SSNs. As Congress continues to propose and consider legislation to protect individuals' personal information, gaps in protections that have already been identified could help focus the debate on the areas that could be addressed immediately based on our work in order to prevent SSNs and other personal information from being misused.

At this Subcommittee's request, we are continuing work on SSNs and the ease with which they can be purchased from Internet information resellers. We look forward to supporting continued congressional consideration of these important policy issues. That concludes my testimony, and I would be pleased to respond to any questions the subcommittee has.

Appendix I: Selected State SSN Laws Previously Reported by GAO

Type of Law	Enacting States
Imposes Limits on State and Local Governments, including Restrictions on Public Disclosure	Connecticut Delaware Florida Georgia Hawaii Indiana Minnesota Nebraska Nevada New Jersey North Dakota Oregon South Carolina Tennessee Texas Virginia West Virginia
Limits Use and Display of SSNs	Arizona Arkansas California Connecticut Georgia Illinois Maryland Michigan Minnesota Missouri Oklahoma Texas Utah Virginia
Limits Use of SSNs on Drivers' Licenses	Indiana North Dakota South Dakota West Virginia
Requires Notification of Security Breaches	California Georgia Nevada New York
Prohibits Certain Activities Related to Identity Theft	Arizona Idaho New York

Appendix I: Selected State SSN Laws Previously Reported by GAO—Continued

Type of Law	Enacting States
Limits or Prohibits Use of SSN as Student ID Number	Arkansas Colorado Wisconsin
Authorizes Redaction of SSNs in Certain Public Records	California New Jersey
Limits Certain Activities of Financial Institutions	North Dakota Vermont
Prohibits Businesses From Requiring SSNs as a Condition of Doing Business	New Mexico Rhode Island
Requires Development of Employee Access Policies	New Mexico
Requires Business to Properly Dispose of Business Records Containing Customers' Personal Information	Texas
Provides Identity Theft Victim Assistance	Washington
Requires that SSNs be Truncated for Certain Public Records	Louisiana
Requires Third Party Contracting Protections	California

Source: GAO Analysis

Related GAO Products

Social Security Numbers: Stronger Protections Needed When Contractors Have Access to SSNs. GAO-06-238. Washington, D.C.: January 23, 2006.

Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain. GAO-05-1016T. Washington, D.C.: September 15, 2005.

Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards. GAO-05-59. Washington, D.C.: November 9, 2004.

Social Security Numbers: Use Is Widespread and Protections Vary in Private and Public Sectors. GAO-04-1099T. Washington, D.C.: September 28, 2004.

Social Security Numbers: Use Is Widespread and Protections Vary. GAO-04-768T. Washington, D.C.: June 15, 2004.

Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information. GAO-04-11. Washington, D.C.: January 22, 2004.

Social Security Numbers: Ensuring the Integrity of the SSN. GAO-03-941T. Washington, D.C.: July 10, 2003.

Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards. GAO-02-352. Washington, D.C.: May 31, 2002.

Social Security: Government and Commercial Use of the Social Security Number is Widespread. GAO/HEHS-99-28. Washington, D.C.: February 16, 1999.

—————

Chairman MCCRERY. Thank you, Ms. Fagnoni. Mr. Winston?

STATEMENT OF JOEL WINSTON, ASSOCIATE DIRECTOR, DIVISION OF PRIVACY AND IDENTITY PROTECTION, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. WINSTON. Mr. Chairman, Mr. Levin, Members of the Subcommittee, I am Joel Winston, Associate Director of the Division of Privacy and Identity Protection at the Federal Trade Commission (FTC). I appreciate the opportunity to testify today about the important issue of SSNs and their relation to identity theft. Although the views expressed in the written testimony represent those of the Commission, my oral presentation and responses to your questions

are my own and do not necessarily represent the opinions of the Commission or any individual Commissioner.

Americans today are very concerned about protecting their identities, and with good reason. Identity theft is a pernicious and persistent problem. When a thief steals your identity, the economic and emotional impact can be severe. American businesses pay a heavy price, as well, as much as \$50 billion every year. Every time consumers hear about the latest data breach that threatens to expose their personal information, they lose a little more confidence in our commercial system.

Access to SSNs contributes to the worst form of identity theft, having new accounts opened in your name. The SSN has become an all-purpose identifier because of its convenience, its uniqueness to each individual, and its permanence over time. Many businesses also use the SSN to authenticate that the person presenting it is who he says he is. It is this dual use that makes the SSN so valuable to identity thieves.

At the same time, the SSN serves many important functions in our financial system. For example, our credit reporting system hinges on the availability of SSNs to match consumers with their financial information. SSNs also are used to locate lost beneficiaries, collect child support, and detect fraud, among many other things.

This presents a challenge, how to find the right balance between permitting beneficial use and disclosure of SSNs while keeping them out of the hands of criminals. The solution must combine a number of approaches. To begin with, public and private entities should use less sensitive identifiers whenever possible and they must do a better job of securing consumer data. This is a fundamental legal responsibility. Under the Federal Trade Commission Act, the Commission can act against firms that misrepresent their security procedures or fail to take reasonable steps to secure sensitive information. The FTC Safeguards Rule requires financial institutions to implement reasonable safeguards to protect consumer information. The FTC Disposal Rule requires businesses that hold certain consumer information to dispose of it in a safe manner.

The Commission has acted aggressively to enforce these legal requirements. Our two most recent cases involved massive data breaches that led to numerous instances of identity fraud. In both cases, the Commission alleged that the company failed to have reasonable procedures to safeguard consumer information, including in one of the cases SSNs.

In addition to law enforcement, education and outreach are critical weapons in this fight. The Commission has targeted its efforts at the three groups best situated to combat identity theft, consumers, industry, and law enforcement. We receive between 15,000 and 20,000 contacts per week from individuals seeking advice on avoiding identity theft or coping with the consequences. We provide information and assistance, including tools to simplify the recovery process.

We are working to implement the provisions of the Fair and Accurate Credit Transactions Act of 2003 Act (P.L. 108-159) (FACT Act), many of which address identity theft. The free annual credit report program, for example, has allowed millions of consumers to

obtain and check their credit reports, where the first signs of identity fraud often appear.

The Commission also works with the business community to promote a culture of security. Our outreach efforts encourage and help businesses to maintain only the information that they need and to protect the information that they maintain.

Finally, the Commission assists criminal law enforcement through our operation of the ID Theft Data Clearinghouse, a national database with over a million identity theft complaints. Law enforcers, ranging from the FBI to local sheriffs, use the clearinghouse to aid in their investigation.

In closing, I want to emphasize that identity theft is a multi-faceted problem for which there is no simple solution. The challenge of determining how best to keep SSNs out of the hands of wrongdoers illustrates how difficult this problem is. Still, there is much that we can do to discourage unnecessary use of SSNs, enhance data protection, educate consumers, and assist criminal prosecutors. The Commission will continue to play a central role in the fight against identity theft and we look forward to working with the Congress in this endeavor.

Thank you again for the opportunity to testify today and I would be happy to answer any questions.

[The prepared statement of Mr. Winston follows:]

Statement of Joel Winston, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission

I. INTRODUCTION

Mr. Chairman, Mr. Levin, and members of the Subcommittee, I am Joel Winston, Associate Director of the Division of Privacy and Identity Protection at the Federal Trade Commission ("FTC" or "Commission").¹ I appreciate the opportunity to present the Commission's views on identity theft and Social Security numbers ("SSNs").

The Commission has a broad mandate to protect consumers generally and to combat identity theft specifically. Controlling identity theft is an issue of critical concern to all consumers—and to the Commission. The FTC serves a key role as the central repository for identity theft complaints, facilitates criminal law enforcement in detecting and prosecuting identity thieves, and provides extensive victim assistance and consumer education. In recognition of the need to protect sensitive consumer information and prevent identity theft, the FTC recently created a new Division of Privacy and Identity Protection. This division—which consists of staff with expertise in privacy, data security, and identity theft—addresses cutting-edge consumer privacy matters through aggressive enforcement, as well as rulemaking, policy development, and outreach to consumers and businesses.

This testimony describes the ways in which SSNs are collected and used, their relationship to identity theft, current laws that restrict the use or transfer of consumers' personal information, and the Commission's efforts to help consumers avoid identity theft or remediate its consequences.

II. THE IDENTITY THEFT PROBLEM

Identity theft is a pernicious crime that harms both consumers and businesses. Recent surveys estimate that nearly 10 million consumers are victimized by some form of identity theft each year.² The costs of this crime are staggering. The Commission's 2003 survey estimated that identity theft cost businesses approximately

¹ The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any Commissioner.

² See *Federal Trade Commission—Identity Theft Survey Report* (2003), <http://www.ftc.gov/os/2003/09/synovatoreport.pdf> and Rubina Johannes, 2006 Identity Fraud Survey Report (2006), <http://www.javelinstrategy.com/research>. A free summary of the 2006 Identity Fraud Survey Report is available at <http://www.bbb.org/alerts/article.asp?ID=651>.

\$50 billion, and cost consumers an additional \$5 billion in out-of-pocket expenses, over the twelve-month period prior to the survey.³ The 2003 survey looked at two major categories of identity theft: (1) misuse of existing accounts; and (2) the creation of new accounts in the victim's name. The 2003 survey found that the costs imposed by new account fraud were substantially higher than the misuse of existing accounts.⁴

III. USES AND SOURCES OF SOCIAL SECURITY NUMBERS

SSNs today play a vital role in our economy. With 300 million American consumers, many of whom share the same name,⁵ the unique 9-digit SSN is a key identification tool for businesses, government, and others.⁶ For example, consumer reporting agencies use SSNs to ensure that the data furnished to them is placed in the correct file and that they are providing a credit report on the correct consumer.⁷ Businesses and other entities use these reports to evaluate the risk of providing to individuals services, such as credit, insurance, home rentals, or employment. Timely access to consumer credit, as well as the overall accuracy of credit reporting files, could be compromised if SSNs could not be used to match consumers to their financial information. Additionally, SSNs are used in locator databases to find lost beneficiaries, potential witnesses, and law violators, and to collect child support and other judgments. SSN databases also are used to fight identity fraud—for example, to confirm that an SSN provided by a loan applicant does not, in fact, belong to someone who is deceased.⁸ Without the ability to use SSNs as a personal identifier and fraud prevention tool, the granting of credit and the provision of other financial services would become riskier and more expensive and inconvenient for consumers.

SSNs are available from both public and private sources. Public records in city and county government offices across the country, including birth and death records, property records, tax lien records, voter registrations, licensing records, and court records, often contain consumers' SSNs.⁹ Increasingly, these records are being placed online where they can be accessed easily and anonymously.¹⁰ There also are a number of private sources of SSNs, including consumer reporting agencies that include name, address, and SSN as part of the "credit header" information on consumer reports. Data brokers also collect personal information, including SSNs, from a variety of sources and compile and resell that data to third parties.¹¹

The misuse of SSNs, however, can facilitate identity theft. For example, new account fraud—the most serious form of identity theft—is often possible only if the thief obtains the victim's SSN. The challenge is to find the proper balance between

³ *Federal Trade Commission—Identity Theft Survey Report* at 6 (2003), <http://www.ftc.gov/os/2003/09/synovatoreport.pdf>.

⁴ *Id.*

⁵ According to the Consumer Data Industry Association, 14 million Americans have one of ten last names, and 58 million men have one of ten first names.

⁶ See General Accounting Office, *Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information* (GAO 04-01) (2004).

⁷ See *Federal Trade Commission—Report to Congress Under Sections 318 and 319 of the Fair and Accurate Credit Transactions Act of 2003* at 38-40 (2004), <http://www.ftc.gov/reports/facta/041209factarpt.pdf>.

⁸ The federal government also uses the SSN as an identifier, for example, as both an individual's Medicare and taxpayer identification number. It also is used to administer the federal jury system, federal welfare and workmen's compensation programs, and military draft registration. See Social Security Administration, *Report to Congress on Options for Enhancing the Social Security Card* (Sept. 1997), www.ssa.gov/history/reports/ssnreportc2.html.

⁹ Local and state governments are reducing their reliance on SSNs for many administrative purposes in response to identity theft concerns. For example, only a few states still use SSNs as drivers license numbers. See David A. Lieb, *Millions of Motorists Have Social Security Numbers on Licenses*, The Boston Globe, Feb. 6, 2006, http://www.boston.com/news/local/massachusetts/articles/2006/02/06/millions_of_motorists_have_social_security_numbers_on_licenses/. In some cases, however, governments still use SSNs as identifiers when it is not essential to do so. See Mark Segraves, *Registering to Vote May Lead to Identity Theft*, WTOP Radio, Mar. 22, 2006, <http://www.wtop.com/?nid=428&sid=733727>.

¹⁰ Improved access to public records has important public policy benefits, but at the same time raises privacy concerns. Some public records offices redact sensitive information such as SSNs, but doing so can be very costly. The Commission has recognized the sensitive nature of SSNs, even when they are contained in publicly available records. For example, in response to a comment on the DSW order, the Commission stated that "[C]ertain publicly available records, such as court records, contain Social Security numbers and other highly sensitive information that can be used to perpetrate identity theft." The Commission response letter is available at <http://www.ftc.gov/os/caselist/0523096/0523096DSW.LettertoCommenterBankofAmerica.pdf>.

¹¹ Some data brokers have announced that they are voluntarily restricting the sale of SSNs and other sensitive information to those with a demonstrable and legitimate need. See *Social Security Numbers Are for Sale Online*, Newsmax.com, Apr. 5, 2005, <http://www.newsmax.com/archives/articles/2005/4/4/155759.shtml>.

the need to keep SSNs out of the hands of identity thieves, while giving businesses and government entities sufficient means to attribute information to the correct person. Restrictions on disclosure of SSNs also could have a broad impact on such important purposes as public health, criminal law enforcement, and anti-fraud and anti-terrorism efforts. Moreover, as referenced above, regulation or restriction of the availability of SSNs in public records poses substantial policy and practical concerns.

IV. CURRENT LAWS RESTRICTING THE USE OF DISCLOSURE OF SOCIAL SECURITY NUMBERS

There are a variety of specific statutes and regulations that restrict disclosure of certain consumer information, including SSNs, in certain contexts. In addition, under some circumstances, entities are required to have procedures in place to ensure the security and integrity of sensitive consumer information such as SSNs. Three statutes that protect SSNs from improper access fall within the Commission's jurisdiction: Title V of the Gramm-Leach-Bliley Act ("GLBA");¹² Section 5 of the Federal Trade Commission Act ("FTC Act");¹³ and the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"),¹⁴ amending the Fair Credit Reporting Act ("FCRA").¹⁵

A. The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act ("GLBA") imposes privacy and security obligations on "financial institutions."¹⁶ Financial institutions are defined broadly as those entities engaged in "financial activities" such as banking, lending, insurance, loan brokering, and credit reporting.¹⁷

1. Privacy of Consumer Financial Information

In general, financial institutions are prohibited by Title V of the GLBA¹⁸ from disclosing nonpublic personal information, including SSNs, to non-affiliated third parties without first providing consumers with notice and the opportunity to opt out of the disclosure.¹⁹ However, the GLBA includes a number of statutory exceptions under which disclosure is permitted without having to provide notice and an opt-out. These exceptions include consumer reporting (pursuant to the FCRA), fraud prevention, law enforcement and regulatory or self-regulatory purposes, compliance with judicial process, and public safety investigations.²⁰ Entities that receive information under an exception to the GLBA are subject to the reuse and redisclosure restrictions of the GLBA Privacy Rule, even if those entities are not themselves financial institutions.²¹ In particular, the recipients may only use and disclose the information "in the ordinary course of business to carry out the activity covered by the exception under which . . . the information [was received]."²²

Entities can obtain SSNs from consumer reporting agencies, generally from the credit header data on the credit report. However, because credit header data is typically derived from information originally provided by financial institutions, entities that receive this information generally are limited by the GLBA's reuse and redisclosure provision.

2. Required Safeguards for Customer Information

The GLBA also requires financial institutions to implement appropriate physical, technical, and procedural safeguards to protect the security and integrity of the information they receive from customers, whether directly or from other financial institutions.²³ The FTC's Safeguards Rule, which implements these requirements for

¹² 15 U.S.C. §§ 6801-09.

¹³ 15 U.S.C. § 45(a).

¹⁴ Pub. L. No. 108-159, 117 Stat. 1952.

¹⁵ 15 U.S.C. §§ 1681-1681x, as amended.

¹⁶ 15 U.S.C. § 6809(3)(A).

¹⁷ 12 C.F.R. §§ 225.28, 225.86.

¹⁸ Privacy of Consumer Financial Information, 16 C.F.R. Part 313 ("GLBA Privacy Rule").

¹⁹ The GLBA defines "nonpublic personal information" as any information that a financial institution collects about an individual in connection with providing a financial product or service to an individual, unless that information is otherwise publicly available. This includes basic identifying information about individuals, such as name, SSN, address, telephone number, mother's maiden name, and prior addresses. *See, e.g.*, 65 Fed. Reg. 33,646, 33,680 (May 24, 2000) (the FTC's Privacy Rule).

²⁰ 15 U.S.C. § 6802(e).

²¹ 16 C.F.R. § 313.11(a).

²² *Id.*

²³ 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule").

entities under FTC jurisdiction,²⁴ requires financial institutions to develop a written information security plan that describes their procedures to protect customer information. Given the wide variety of entities covered, the Safeguards Rule requires a plan that accounts for each entity's particular circumstances—its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. It also requires covered entities to take certain procedural steps (for example, designating appropriate personnel to oversee the security plan, conducting a risk assessment, and overseeing service providers) in implementing their plans.²⁵

B. Section 5 of the FTC Act

Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.”²⁶ Under the FTC Act, the Commission has broad jurisdiction over a wide variety of entities and individuals operating in commerce. Prohibited practices include making deceptive claims about one's privacy procedures, including claims about the security provided for consumer information.²⁷

In addition to deception, the FTC Act prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition.²⁸ The Commission has used this authority to challenge a variety of injurious practices, including companies' failure to provide reasonable and appropriate security for sensitive customer data.²⁹ The Commission can obtain injunctive relief for violations of Section 5, as well as consumer redress or disgorgement in appropriate cases.

C. The Fair and Accurate Credit Transactions Act of 2003

The FACT Act amended the FCRA to include a number of provisions designed to increase the protection of sensitive consumer information, including SSNs. One such provision required the banking regulatory agencies, the NCUA, and the Commission to promulgate a coordinated rule designed to prevent unauthorized access to consumer report information by requiring all users of such information to have reasonable procedures to dispose of it properly and safely.³⁰ This Disposal Rule, which took effect on June 1, 2005, should help minimize the risk of improper disclosure of SSNs.

In addition, the FACT Act requires consumer reporting agencies to truncate the SSN on consumer reports at the consumer's request.³¹ Eliminating the unnecessary display of this information could lessen the risk of it getting into the wrong hands.

²⁴ The Federal Deposit Insurance Corporation, the National Credit Union Administration (“NCUA”), the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Office of Thrift Supervision, and state insurance authorities have promulgated comparable information safeguards rules, as required by Section 501(b) of the GLBA. 15 U.S.C. § 6801(b); see, e.g., Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8,616–41 (Feb. 1, 2001). The FTC has jurisdiction over entities not subject to the jurisdiction of these agencies.

²⁵ The Commission previously has recommended that Congress consider whether companies that hold sensitive consumer data, for whatever purpose, should be required to take reasonable measures to ensure its safety. Such a requirement could extend the FTC's existing GLBA Safeguards Rule to companies that are not financial institutions. See Statement of Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft (June 16, 2005) at 7, <http://www.ftc.gov/os/2005/06/050616databreaches.pdf>.

²⁶ 15 U.S.C. § 45(a).

²⁷ Deceptive practices are defined as material representations or omissions that are likely to mislead consumers acting reasonably under the circumstances. *Cliffdale Associates, Inc.*, 103 F.T.C. 110 (1984).

²⁸ 15 U.S.C. § 45(n).

²⁹ Other practices include, for example, allegations of unauthorized charges in connection with “phishing,” high-tech scams that use spam or pop-up messages to deceive consumers into disclosing credit card numbers, bank account information, SSNs, passwords, or other sensitive information. See *FTC v. Hill*, No. H 03–5537 (filed S.D. Tex. Dec. 3, 2003), <http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm>; *FTC v. C.J.*, No. 03–CV–5275–GHK (RZX) (filed C.D. Cal. July 24, 2003), <http://www.ftc.gov/os/2003/07/phishingcomp.pdf>.

³⁰ 16 C.F.R. Part 382 (“Disposal of Consumer Report Information and Record Rule”).

³¹ 15 U.S.C. § 1681g(a)(1)(A). The FTC advises consumers of this right through its consumer outreach initiatives. See e.g., the FTC's identity theft prevention and victim recovery guide, *Take Charge: Fighting Back Against Identity Theft* at 5 (2005), available at <http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf>.

D. Other Laws

Other federal laws not enforced by the Commission regulate certain other specific classes of information, including SSNs. For example, the Driver's Privacy Protection Act ("DPPA")³² prohibits state motor vehicle departments from disclosing personal information in motor vehicle records, subject to fourteen "permissible uses," including law enforcement, motor vehicle safety, and insurance. The Health Information Portability and Accountability Act ("HIPAA") and its implementing privacy rule prohibit the disclosure to third parties of a consumer's medical information without prior consent, subject to a number of exceptions (such as, for the disclosure of patient records between entities for purposes of routine treatment, insurance, or payment).³³ Like the GLBA Safeguards Rule, the HIPAA Privacy Rule also requires entities under its jurisdiction to have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."³⁴

E. FTC Enforcement Actions

Over the past year or so, reports have proliferated about information compromises at U.S. businesses, universities, government agencies, and other organizations that collect and store sensitive consumer information, including SSNs. Some of these incidents reportedly have led to identity theft, confirming that security breaches can cause real and tangible harm to consumers, businesses, and other institutions.

Since 2001, the Commission has brought twelve cases challenging businesses that have failed to take reasonable steps to protect sensitive consumer information in their files.³⁵ Two of the Commission's most recent law enforcement actions arose from high-profile data breaches that occurred last year. In the first case, the Commission alleged that a major data broker, ChoicePoint, Inc., failed to use reasonable procedures to screen prospective subscribers and monitor their access to sensitive consumer data, in violation of the FCRA³⁶ and the FTC Act.³⁷ The Commission's complaint alleged that ChoicePoint's failures allowed identity thieves to obtain access to the personal information of over 160,000 consumers, including nearly 10,000 consumer reports. In settling the case, ChoicePoint agreed to pay \$10 million in civil penalties for the FCRA violations—the highest civil penalty ever levied in a consumer protection case—and \$5 million in consumer redress for identity theft victims. The Order also requires ChoicePoint to implement a number of strong data security measures, including bi-annual audits to ensure that these security measures are in place.

In the second action, the Commission reached a settlement with CardSystems Solutions, Inc., the card processor allegedly responsible for last year's breach of credit and debit card information for Visa and MasterCard, which exposed tens of millions of consumers' credit and debit numbers.³⁸ This case addresses the largest known compromise of sensitive financial data to date. As in the ChoicePoint case, the FTC alleged that CardSystems engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive consumer data. These settlements provide important protections for consumers and also provide important lessons for industry about the need to safeguard consumer information.

V. THE COMMISSION'S EFFORTS TO COMBAT IDENTITY THEFT

In addition to our efforts to ensure that businesses take reasonable steps to safeguard sensitive consumer information, the Commission works in many other ways to address the identity theft problem. Pursuant to the 1998 Identity Theft Assump-

³² 18 U.S.C. §§ 2721–25.

³³ 45 C.F.R. Part 164 ("HIPAA Privacy Rule").

³⁴ 45 C.F.R. § 164.530(c).

³⁵ Documents related to these enforcement actions generally are available at <http://www.ftc.gov/privacy/index.html>.

³⁶ 15 U.S.C. §§ 1681–1681x, as amended. The FCRA specifies that consumer reporting agencies may only provide consumer reports for certain "permissible purposes." ChoicePoint allegedly approved as customers individuals whose applications had several indicia of fraud, including false credentials, the use of commercial mail drops as business addresses, and multiple applications faxed from the same public commercial location. The FTC's complaint alleged that ChoicePoint did not have a permissible purpose in providing consumer reports to such individuals and failed to have reasonable procedures to verify prospective subscribers.

³⁷ *United States v. ChoicePoint, Inc.*, No. 106–CV–0198 (N.D. Ga. Feb. 15, 2006).

³⁸ In the Matter of CardSystems Solutions, Inc., FTC File No. 052–3148 (proposed settlement posted for public comment, Feb. 23, 2006). The settlement requires CardSystems and its successor corporation to implement a comprehensive information security program and obtain audits by an independent third-party professional every other year for 20 years. As noted in the FTC's press release, CardSystems faces potential liability in the millions of dollars under bank procedures and in private litigation for losses related to the breach.

tion and Deterrence Act ("the Identity Theft Act"),³⁹ the Commission has implemented a program that assists consumers, businesses, and other law enforcers.

A. Working with Consumers

The Commission hosts a toll-free hotline, 1-877-ID THEFT, and a secure online complaint form on its website, www.consumer.gov/idtheft, for consumers concerned about identity theft. Every week, the Commission receives about 15,000 to 20,000 contacts from victims and consumers seeking information on how to avoid identity theft. The callers to the hotline receive counseling from trained personnel who provide information on steps they can take both to prevent identity theft and to resolve problems resulting from the misuse of their identities. Victims are advised to: (1) obtain copies of their credit reports and have a fraud alert placed on them;⁴⁰ (2) contact each of the creditors or service providers with which the thief has established or accessed an account to request that the account be closed and to dispute any associated charges; and (3) report the theft to the police and, if possible, obtain a police report. The police report is useful in demonstrating to purported creditors and debt collectors that the consumer is a victim of identity theft, and serves as an "identity theft report" that can be used for exercising various victims' rights granted by the FACT Act.⁴¹ The Commission's identity theft website, www.consumer.gov/idtheft, has an online complaint form where victims can enter their complaints into the Clearinghouse.

The Commission also has taken the lead in developing and disseminating identity theft-related consumer education materials, including an identity theft primer, *ID Theft: What It's All About*, and a victim recovery guide, *Take Charge: Fighting Back Against Identity Theft*. The Commission alone has distributed more than 2.1 million copies of the *Take Charge* booklet (formerly known as *ID Theft: When Bad Things Happen To Your Good Name*) since its release in February 2000 and has recorded more than 2.4 million visits to the Web version. The Commission also maintains the identity theft website, www.consumer.gov/idtheft, which provides publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources.

Last fall, the Commission, together with partners from law enforcement, the technology industry, and nonprofits, launched OnGuard Online, an interactive, multimedia resource for information and up-to-the minute tools on how to recognize Internet fraud, avoid hackers and viruses, shop securely online, and deal with identity theft, spam, phishing, and file-sharing.⁴²

In addition, the Commission will launch this spring a major new identity theft education campaign. The campaign will encourage consumers to guard against identity theft by taking steps to reduce their risk, keep a close eye on their personal information, and move quickly to minimize the damage if identity theft occurs. The centerpiece of the campaign will be a turnkey toolkit—a comprehensive how-to guide that will help promote grassroots education about identity theft.

The Commission also has developed ways to simplify the recovery process. One example is the ID Theft Affidavit, included in the *Take Charge* booklet and on the website. This standard form was developed in partnership with industry and consumer advocates for victims to use in resolving identity theft debts. To date, the Commission has distributed more than 293,000 print copies of the Affidavit and has recorded more than 1.1 million hits to the Web version.

B. Working with Industry

The private sector can play a key role in combating identity theft by reducing its incidence through better security and authentication. The Commission works with institutions to promote a "culture of security" by identifying ways to spot risks to the information they maintain and keep it safe.

³⁹ Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

⁴⁰ The FACT Act added a requirement that consumer reporting agencies, at the request of a consumer, place a fraud alert on the consumer's credit report. Consumers may obtain an initial alert if they have a good faith suspicion that they have been or are about to become an identity theft victim. The initial alert must stay on the file for at least 90 days. Actual victims who submit an identity theft report can obtain an extended alert, which remains in effect for up to seven years. Fraud alerts require users of consumer reports who are extending credit or related services to take certain steps to verify the consumer's identity. See 15 U.S.C. § 1681c-1.

⁴¹ These include the right to an extended fraud alert, the right to block fraudulent trade lines on credit reports and to prevent such trade lines from being furnished to a consumer reporting agency, and the ability to obtain copies of fraudulent applications and transaction reports. See 15 U.S.C. § 1681 *et seq.*, as amended.

⁴² See www.onguardonline.gov. OnGuard Online is also available in Spanish. See www.AlertaEnLinea.gov.

Among other things, the Commission has disseminated advice for businesses on reducing risks to their computer systems⁴³ and on compliance with the Safeguards Rule.⁴⁴ Our emphasis is on preventing breaches before they happen by encouraging businesses to make security part of their regular operations and corporate culture. The Commission also has published *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, a booklet on managing data compromises.⁴⁵ This publication provides guidance on when it would be appropriate for an entity to notify law enforcement and consumers in the event of a breach of personal information.

In 2003, the Commission held a workshop that explored the challenges consumers and industry face in securing their computers. Titled "Technologies for Protecting Personal Information: The Consumer and Business Experiences," the workshop also examined the role of technology in meeting these challenges.⁴⁶ Workshop participants, including industry leaders, technologists, researchers on human behavior, and representatives from consumer and privacy groups, identified a range of challenges in safeguarding information and proposed possible solutions.

C. Working with Law Enforcement

A primary purpose of the Identity Theft Act was to provide law enforcement with access to a centralized repository of identity theft victim data to support their investigations. The Commission operates this database as a national clearinghouse for complaints received directly from consumers and through numerous state and federal agencies, including the Social Security Administration's Office of Inspector General.

With over 1,060,000 complaints, the Clearinghouse provides a detailed snapshot of current identity theft trends as reported by the victims themselves. The Commission publishes data annually showing the prevalence of complaints broken out by state and city.⁴⁷ Since its inception, nearly 1,400 law enforcement agencies have registered for access to the Clearinghouse database. Individual investigators within those agencies can access the system from their desktop computers 24 hours a day, seven days a week. The Clearinghouse also gives access to training resources, and enables users to coordinate their investigations.

The Commission also encourages use of the Clearinghouse through training seminars offered to law enforcement. In cooperation with the Department of Justice, the U.S. Postal Inspection Service, the U.S. Secret Service, and the American Association of Motor Vehicle Administrators, the Commission began organizing full-day identity theft training seminars for state and local law enforcement officers in 2002. To date, this group has held 20 seminars across the country. More than 2,880 officers have attended these seminars, representing over 1,000 different agencies. Future seminars are being planned for additional cities.

To further assist law enforcers, the Commission staff developed an identity theft case referral program. The staff creates preliminary investigative reports by examining patterns of identity theft activity in the Clearinghouse, and refers the reports to financial crimes task forces and others for further investigation and possible prosecution. In addition, analysts from the FBI, U.S. Secret Service, and Postal Inspection Service work on-site at the FTC, developing leads and supporting ongoing investigations for their agencies.

VI. CONCLUSION

The crime of identity theft is a scourge, causing enormous damage to businesses and consumers. The unauthorized use of consumers' SSNs is an important tool of identity thieves, especially those seeking to create new accounts in the victim's name. Although current laws place some restrictions on the use or disclosure of SSNs by certain entities under certain circumstances, this information is still other-

⁴³ *Security Check: Reducing Risks to Your Computer Systems*, available at <http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm>.

⁴⁴ *Financial Institutions and Customer Data: Complying with the Safeguards Rule*, available at <http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm>.

⁴⁵ *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, available at <http://www.ftc.gov/bcp/conline/pubs/buspubs/identityrespond.pdf>.

⁴⁶ See workshop agenda and transcripts available at www.ftc.gov/bcp/workshops/technology. See Staff Report available at <http://www.ftc.gov/bcp/workshops/technology/finalreport.pdf>.

⁴⁷ See *Federal Trade Commission—National and State Trends in Fraud & Identity Theft* (Jan. 2006), available at <http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf>. The Commission also conducts national surveys to learn how identity theft impacts the general public. The FTC conducted the first survey in 2003 and is conducting a second survey this spring. See *Federal Trade Commission—Identity Theft Survey Report* (Sept. 2003), available at <http://www.ftc.gov/os/2003/09/synovaterreport.pdf>.

wise available from both public and private sources, thereby enabling identity thieves to obtain SSNs through legal means as well as illegal means.

At the same time, SSNs are an important driver of our market system. Businesses and others rely on SSNs to provide many important benefits for consumers and to fight identity theft.

There are a number of things that government, industry, and consumers can do to help stem the tide of identity theft. First, both government and industry need to consider what information they collect and maintain from or about consumers and whether they need to do so. Entities that possess sensitive consumer information should continue to enhance their procedures to protect it. The Commission will continue its law enforcement and outreach efforts to encourage and, when necessary, require better protections.

Second, industry should continue the development of improved fraud prevention methods to stop identity thieves from misusing the consumer information they have managed to obtain. In this regard, the FACT Act should prove instrumental by requiring the bank regulatory agencies, the NCUA, and the FTC to develop jointly regulations and guidelines for financial institutions and creditors to identify possible risks of identity theft.⁴⁸

Third, the Commission will continue and strengthen its efforts to empower consumers by providing them with the knowledge and tools to protect themselves from identity fraud and to deal with the consequences when it does occur. As discussed above, new consumer rights granted by the FACT Act should help consumers minimize the damage.

Finally, the Commission will continue to assist criminal law enforcement in detecting and prosecuting identity thieves. The prospect of serious jail time hopefully will discourage those considering identity theft from perpetrating this crime.

The Commission looks forward to continuing to work with Congress to address ways to reduce identity theft.

Chairman MCCRERY. Thank you, Mr. Winston. Can you fill us in on what your agency does specifically to try to ensure compliance with the laws that you talked about in your testimony that fall in your jurisdiction?

Mr. WINSTON. Well, we go about it in many ways. First and foremost, we are a law enforcement agency and we investigate and take action against companies that violate the laws that we enforce, for example, cases against companies that fail to safeguard information that they have. We brought 12 cases to date. We have a number of others under investigation. I think we have sent a pretty clear message to the business community that this is an important requirement.

At the same time, we are strong believers in education, both for businesses and consumers. That is always the first line of defense and we work very hard in that regard.

Chairman MCCRERY. Ms. Fagnoni, you talked about the fact that many States have enacted laws that restrict the use of SSNs. Can you give us an idea of how those actions by States affect businesses and commerce in those States and maybe even how it affects businesses and commerce across the country?

Ms. FAGNONI. The work we did, we had more information about the impacts on different government activities and the ease of getting information. One example of how business and commerce has been affected by these laws is that, particularly when a State like California, a large State such as California enacts a law, for example, the law where any entity where there is a security breach involving information, private information, personal information from

⁴⁸ 15 U.S.C. § 1681m(e).

somebody who resides in the State of California, the California law is that those individuals have to be notified. Some large companies now have on that basis made it a practice to notify anyone when there is a security breach, regardless of what State they happen to live in, based on, perhaps the pressure and the precedent in having certain laws in place.

That is one example where companies have had to adapt and adjust to some of those laws. Having different laws in different States probably can also cause some challenges for people who do business in multiple jurisdictions. As I said, a lot of what our studies have shown is that once, whether it is government or private entities become more aware of the ways in which the SSN can be fraudulently used and they start to take actions on their own to better secure the information, they can still continue to use the SSN for the purposes that are very important to commerce. They have a better sense and a clear understanding of the need to protect the exposure of that number beyond the uses for which it is needed.

Chairman MCCRERY. Thank you. Would you talk a little bit about the Internet and the availability of SSNs on the Internet? Should we be looking at some new Federal laws regarding public display of SSNs?

Ms. FAGNONI. In the work we did looking at government and selected private sector use of SSNs, we did not find a large percentage of entities that were placing the SSNs on the Internet, particularly in the local and State government levels. Most of the information that is publicly available through those entities is on paper or microfiche or microfilm and people actually have to go to a location, such as a courthouse or someplace like that, and actually look for the information.

We do have some work ongoing right now where we are looking at the information resellers who are selling information via the Internet and we will have some information to report fairly soon on that. It does raise some questions about how carefully some information sellers are paying attention to who is actually asking for the information and what kinds of safeguards are in place to ensure that the information is being provided only to those where it is an appropriate use.

Chairman MCCRERY. Thank you. Mr. Becerra?

Mr. BECERRA. Thank you, Mr. Chairman, and thank you to the two of you for your testimony.

Let me ask a question and revert back to the testimony of our two colleagues who were just here and talked about using the SSN for purposes of trying to determine one's eligibility to work in this country. Any comments on what you heard in the discussion that took place among the Members on that particular proposal?

Ms. FAGNONI. We don't really have work that would comment on it directly, but there is a difference. First of all, they were talking about having a card that was tamper-proof, and there are all sorts of issues associated with looking at the different options and what would be appropriate and what the cost would be.

There also is an issue which somebody raised about the information on the card which is only going to be as good as the information in the databases in DHS and SSA. We have reported on the fact that to the extent that, for example, information about some-

body's visa status, if that is not kept up to date and isn't updated somehow through the encryption, then that is going to limit the usefulness of the database.

There is a whole separate issue on the deterrent effect, which I really can't comment on.

Mr. BECERRA. Okay.

Mr. WINSTON. I found the discussion very interesting and I thought the point that you made actually was the one that I was thinking of, as well, and that is you can have a national number for immigrants or even for citizens, but any time you have a number that is the key to benefits, it is going to potentially be something that is valuable to identity thieves. The trick is to find a way of identifying people and authenticating who they are without having that information get in the hands of the wrongdoers and that is a very difficult task.

Mr. BECERRA. As we explore how we can better protect the SSN, is there something that we have learned in these examinations about best practices or what some either public or private sector agencies, enterprises are doing to try to protect the number, anything that you can tell us that can help us with regard to this ongoing examination?

Ms. FAGNONI. Keying off Mr. Winston's testimony, in the work we did where we looked at four sectors—banking, financial institutions, telecommunications, and tax preparers—it was clear that because of the laws and the regulatory structure surrounding the banking and financial institutions industries, there are a lot more protections in place regarding the protection of personal information, including the SSN.

Particularly in telecommunications, there really are no laws that are designed to explicitly ensure that telecommunications companies are protecting SSNs. The companies are relying on individual contracts and things like that.

As a matter for the Congress, one option would be to look at regulatory structures in terms of protecting information and consider whether or not those could be more broadly applied, or conversely, to look at some other specific sectors that don't now have laws in place that might warrant them.

Mr. BECERRA. Let me ask just one last question, and if you wish to comment on something else, that is fine so long as I have time. I am not sure how to phrase it. Do we need to have one identifier, or should we ask all these various industries to have their own identifiers? The banking industry or financial services, you all keep an identifier that is for your purposes. Credit bureaus, those who are checking status of your demographic, your activities, whether purchasing or doing anything else, you keep your own number. The Federal Government, you keep your own number. State, driver's license and all the rest, you keep your own number.

Should we have one, or should we, for purposes of trying to make sure we don't have a number that can be stolen or has that value if it is stolen, should we try to move toward something that says, you all keep your own numbers and that way no one can steal that much value from an individual when they get that identifier?

Ms. FAGNONI. The reason the SSN is so valuable is because often, and I am sure you will hear this from the next panel, some-

body who is trying to check somebody's credit or make sure that the individual they are talking to is the appropriate person and they should be sharing certain information, the only way they can ensure somebody's identity, looking across different kinds of pieces of information, is through that common identifier, the SSN.

At the same time, though, we have a lot of examples where more and more kinds of entities are moving away from the display of the SSN. I think there is a difference between needing it and protecting it because it is a very important way to protect against fraud. At the same time, whether it is a driver's license or a health care card or whatever, over the past several years cards that routinely used SSNs now either first voluntarily and then now routinely across the board use other special identifiers unique to that particular entity for display purposes. They still have that SSN, behind the scenes that they need for data matching and things like that.

Mr. WINSTON. I would just add very briefly, I agree with that, and there is a lot we can do to convince people to stop using SSNs when they don't need to, but at the same time, we have to look at the back end, and the back end is somebody appears before you with an SSN and wants to take out a loan. How do you make sure that person is who he says he is? It is the fact that the SSN is being used for that purpose, as well as for the identification purpose, that creates the problem. That is the key that unlocks the door to identity theft. The more we can go to systems of passwords, PINs, and get away from using the SSN as the authenticator, I think the better we will be.

Mr. BECERRA. Thank you. Thanks very much, Mr. Chairman.
Chairman MCCRERY. Mr. Brady?

Mr. BRADY. Thank you, Mr. Chairman. A couple of questions, three, really. The first two are fairly direct. Identity theft is such a big issue. What percentage, would you guess, of identity thefts start with a stolen SSN?

Mr. WINSTON. I can talk about the surveys we have done and that others have done, which indicate that about two-thirds of identity theft is what is called account takeover, and that is where somebody gets your credit card number or your bank card number and gets into your account. Typically, that doesn't require an SSN to do.

The other one-third is new account fraud, where they actually go out and open a new account in your name. Typically, although not always, typically, you need an SSN to do that kind of fraud. It is about one-third.

Mr. BRADY. That leads right to the second question. What is the most common way of obtaining a stolen SSN? Is it a stolen card? Is it mail theft, computer hacking, information resellers? What is the most common of those, would you guess?

Mr. WINSTON. It is a little hard to tell from the surveys because most people don't know how their identity was stolen in the first place. They just know it happened. They don't know who did it. They don't know how it got done. If you look at just the data for people who do know what happened, you find that most of it is done through lost wallets or friends, relatives who get a hold of your information. That is not necessarily representative of half or

more of the people who don't know. There are a lot of potential sources. It is really hard to tell what is the biggest.

Mr. BRADY. A final question. Part of the, I think, complexity is the issue of information resellers. Even if we are able to sort of contain this issue at the source, as it gets sold, integrity becomes less and loose and things happen. I will ask both of you, who is responsible for ensuring that information resellers and financial institutions and those to whom they sell SSNs only disclose according to the law and who monitors it and what kind of resource do we use to tackle that problem?

Ms. FAGNONI. Well, quickly, initially, who has authority, if anyone, is dependent on what industry is involved, and that is where we found, at least of the four industries we looked at and other examples we have, it varies. It is based on the laws that regulate that particular industry.

In some cases, information resellers, for example, consider themselves to be financial institutions and therefore subject to the different kinds of laws regulating that industry. In other cases, they don't and it is honestly not clear if there is any regulatory framework.

Mr. WINSTON. Just to elaborate on that, generally speaking, resellers get SSNs from credit bureaus. Credit bureaus get it from financial institutions. That is subject to the Gramm-Leach-Bliley Act (P.L. 106-102). There are restrictions on people who buy information from resellers in how they can use—how they can get the information and how they can use it. We are responsible for enforcing that law as to the non-bank entities. The banking agencies are responsible for the banks.

Mr. BRADY. How much resource do you put toward that?

Mr. WINSTON. We have a new division at the FTC, the Division of Privacy and Identity Protection, which is devoted solely to issues of identity theft, consumer privacy, ensuring that consumer information is protected. We have a staff of about 30 people who are looking at these issues and enforcing the law.

Mr. BRADY. For your agency, can you guess or do you know how many businesses have been investigated, information resellers, for example, or businesses using it fraudulently have been investigated and successfully prosecuted?

Mr. WINSTON. There have been a number, but the most recent case against Choice Point is a good example.

Mr. BRADY. Sure.

Mr. WINSTON. Choice Point is one of the largest data brokers in the country and they didn't have procedures in place to ensure that the people who called them up to buy SSNs and other information were legitimate. As a result—

Mr. BRADY. Thankfully, that got a lot of attention, but are we talking about thousands of businesses across the country are investigated, hundreds are investigated, dozens are investigated?

Mr. WINSTON. Keep going.

[Laughter.]

Mr. BRADY. Getting a little smaller, isn't it.

Mr. WINSTON. We are a small agency. I don't know what the number would be. It is certainly not in the hundreds or thousands. That is all we can—that is all that we have the resources to do.

Mr. BRADY. Thank you, Mr. Chairman, and thank you, both panelists.

Ms. FAGNONI. Thank you.

Chairman MCCRERY. Thank you, Ms. Fagnoni. Thank you, Mr. Winston.

Our next panel is Nicole Robinson, North Atlantic Coast Volunteer Coordinator, Identity Theft Resource Center, San Diego, California; Mary McQueen, on behalf of the Council of State Court Administrators, Williamsburg, Virginia; Erik Stein, member of BITS Fraud Reduction Steering Committee; Stuart Pratt, President and CEO of Consumer Data Industry Association; and Bruce Hulme, Legislative Director, National Council of Investigation and Security Services from New York. Welcome, everybody.

The same rules apply. Your written statements will be included in the record in their entirety, but we would ask you to summarize those statements in about 5 minutes.

We will begin, Ms. Robinson, with you. Thank you for coming. You may begin.

STATEMENT OF NICOLE ROBINSON, NORTH ATLANTIC COAST VOLUNTEER COORDINATOR, IDENTITY THEFT RESOURCE CENTER, SAN DIEGO, CALIFORNIA

Ms. ROBINSON. Good afternoon, Mr. Chairman, Members of the Committee. Thank you for the opportunity to testify on behalf of this very important topic.

My name is Nicole Robinson, and besides being the North Atlantic Coast Coordinator for the Identity Theft Resource Center, I am also a victim of identity theft, and I want to start first off to tell you—try to be brief about my identity theft case.

It first started in 2000 and I was notified by a fraud investigator, Kay Jewelers said someone had used my SSN to open an instant credit account. That first night, she bought watches and a ring totaling \$2,300. The next night, she came trying to max out the account and they were alerted to it because people don't usually do that with jewelry store accounts.

Well, I contacted the three credit reporting agencies on that Monday. It was very difficult to get my credit reports because she had used different addresses in Texas and I couldn't get my own credit reports. I soon came to find out that she had applied for a personal loan at my mortgage lender. She was picked up by the Bear County police getting a personal check in my name. My mortgage lender never contacted me, although they knew they held a mortgage for me in Maryland and she was in Texas. The police let her go that day. She promised that she wouldn't do it again. She cried. She said she didn't know what she was doing was wrong and they let her go home.

After that, since she knew I had a mortgage, she applied for a mortgage several days later. She continued to apply for credit, even though she had been picked up by the police. She, in a 3 month period, got \$36,000 in goods and services. She had a Geico car insurance policy in my name and Geico would not give me the VIN number off the vehicle so I could track back to the dealership that sold it because they said they had to protect her privacy.

As time went on, she was eventually indicted and she pled guilty to two counts of misusing my identifying information. She served no time in jail. She was ordered to pay restitution. I have only seen a small portion of the restitution thus far.

As time has gone, I have borne the burden of her theft of my identity. I continue to get her collection notices at my home in Maryland. As recently as last summer, I got a collection notice from a collection agency where Nicole Robinson—and that is her name, her name is Nicole Robinson, as well—she had gone to a dentist in Texas while she was in police custody and had a tooth extracted. Well, of course she didn't pay for it and so the collection agency started to look for her. Instead of finding her in Texas, they sent a collection notice to my home in Maryland.

I have continued to get collection notices for bad checks that she has written. I also get preapproved credit card offers at my home in her name, and the only reason why I know it is for her is because we have a different middle initial and they always come with her middle initial.

As I started to get my credit reports, in 2004, I got a 54-page credit report. It had 170 accounts on it. A hundred-and-thirty of them were in collections. It had 42 different names and 65 different addresses. I was notified by another credit reporting agency that my SSN resided on five different credit reports.

Even as recently as this year, when a mortgage broker ran my credit report, her bad debts, even a judgment from an apartment complex in Texas, is on my credit report, and it is not on the credit reports that the credit reporting agency sends to me, but it is on the credit report that they disclose to the lenders.

As a result of me being a victim of identity theft, I do speak to consumer groups about protecting your SSN. The way my SSN was stolen by Nicole Robinson is that she worked for a business called Care Mark, and Care Mark used to provide mail-in pharmaceutical services for a law firm where I used to work. Even though I was no longer an employee of the law firm, she still had access to my information in their databases. I ultimately found out that she used the SSN of several people named Nicole Robinson and she was able to get cars and jewelry, and when she bought a vacuum cleaner, somebody reported to the police in Texas that she had a warehouse full of stuff that she had stolen.

I just want to go over briefly some of the recommendations from the Identity Theft Resource Center on securing data. We realize that businesses do use the SSN. It is so much a part of what a lot of businesses do. We think that businesses should take extra precautions to secure the SSN.

In my case, Nicole Robinson had access to my SSN years after I was a member of the health plan that required me to use my SSN as an identifier. She should have never had access to that number because I was no longer a member of that plan. Even if she had access to my records, my SSN should have been redacted in whole or in part.

We believe that consumer education is key. A lot of people don't see the risk in carrying their Social Security cards in their wallets and we believe that when you get your annual statement from the

SSA, there should be a consumer alert on there about protecting your SSN.

We also believe that businesses should assume responsibility for the protection of your SSN. If they require it, they should also protect it.

Thank you very much.

[The prepared statement of Ms. Robinson follows:]

**Statement of Nicole Robinson, North Atlantic Coast Volunteer Coordinator,
Identity Theft Resource Center, San Diego, California**

Members of the committee: Thank you for the opportunity to provide both written and oral testimony for your committee today and for your interest in the topic of identity theft.

The oral portion of our testimony will be provided by Nicole Robinson, a survivor of identity theft, and the highest ranking ITRC volunteer on North Atlantic Coast.

The nonprofit Identity Theft Resource Center (ITRC) is passionate about combating identity theft, empowering consumers and victims, assisting law enforcement, reducing business loss due to this crime and helping victims. We also realize that you are in a difficult position of trying to impose laws that may impact consumers, business and government.

However, ITRC firmly believes that it is possible to find a balance between the creation of strong identity theft laws to protect consumers and businesses and allowing the business community to flourish and grow. It is critical that all parties be considered in any legislation you pass and in all of your deliberations. After all—In each case of Financial Identity Theft there are at least two sets of victims—the individual whose SSN was used and the business that has lost services, goods or money. We all victims of this crime and we appreciate your time in addressing this issue.

We are honored by your invitation and will continue to make our opinions available upon request to your representatives over the next few months as you grapple with this complex crime and its many issues.

Introduction:

Governmental agencies at all levels, businesses and consumers have for ease and convenience tied and associated many critical elements of daily life to the individual Social Security Number (SSN). The individual number is the primary key to the individual's credit history, work history education and health information. You must have one to work, gain tenancy, credit and to identify individuals on tax forms.

More and more business and entities are collecting personal information about each and every one of us. These can range from your bank to the soccer league that your child plays in. Add to that number the schools where you or your child attended, all the job applications you have ever filled out, the Funeral Home that is preplanning your final arrangements and the many health facilities that you have used. Some veterinarians, self-storage units and even car rental companies ask for SSNs.

In some cases there is a valid reason to collect the information and the Identity Theft Resource Center holds that it should be allowed to continue. Our concern lies not in the collection of the Social Security number but in the use, storage, access and misuse of this key information.

It must be noted that the crime of identity theft is not a particularly new crime. It is more that in the current environment of electronic credit and business identity theft has become extremely profitable and safe for the thief. The thief faces little chance of apprehension with minimal penalties for the theft of thousands of dollars.

Each day the thieves grow more accomplished at their task. Now it is time for businesses, governmental agencies and consumers to adopt a more proactive position on the value of the Social Security number as a marketable commodity. Consumers need to realize it has value. Businesses and governmental entities need to accept responsibility for this item of value, the Social Security number. We need to create a plan that focuses on all involved parties and not just on the business community.

Numerous surveys have proven that consumers do not feel trust for companies or the government proactively protecting their personal identifying information. They believe, with cause, their information is accessible to too many people and handled without protection. In order to increase customer, employee and client trust, new security processes must be implemented as soon as possible.

Findings and Recommendations:

SSN as an identifier on items in wallets

Finding: Too many people carry their Social Security number on their person, in the form of the actual Social Security card, health insurance cards, Military ID cards, employee id cards or Medicare/Medical cards and driver's license numbers. Wallets are primary targets by identity thieves, pickpockets and drug addicts who hope to profit this information.

Recommendation: The Social Security number should *not* be used as an identifier in any circumstances and should never be on cards carried in the wallet, even on the magnetic strip due to improvements in skimming technology. Randomized numbering systems should be used that match the SSN in a well-protected database when necessary such as for Medicare benefits.

Consumer Education

Recommendation: That all Social Security cards come with an advisory with the original card and that this advisory should also be sent out yearly with the person's work benefit statement. This advisory should include under what circumstances one should give out a SSN, when not to, a telephone number to call with questions or to file complaints, and not to carry a SS card in one's wallet, palm pilot or laptop.

Recommendation: That the SSA work with other governmental and private entities to continue to educate consumers about scams that involve the SSN. A study of the SSA site only included one scam warning as the beginning of March 2006.

Overcollection/misuse of the SSN

Recommendation: Too many companies are unnecessarily asking for a person's SSN. While it may not be practical to limit the collection of the SSN, a blanket liability should be incurred all entities that collect this information from an individual or secondary source. It is not unreasonable for any individual to expect basic standards of protection of the information obtained by the entity doing the collection. Federal, state and private right of actions should included in any bill considered in order for there to be effective encouragement to self-enforce these standards.

Information Security

Finding: The number of publicized security breaches during 2005 clearly indicates a serious problem. Whereas it is not possible to build an impenetrable security system around data, it is clear that companies and governmental agencies need to have a tighter control on information. This rule cannot just apply to businesses. All governmental agencies need to be held to the same standard and be a leader in this movement.

Recommendation: Companies and all levels of governmental agencies should be required to do an information risk assessment of both paper and electronic documents containing a Social Security number. This assessment should include the ability to follow information from the point of entry to beyond disposal, including the auditing of any person, department or storage space. A written policy should be designed that limits access to the SSN, describes the protection of the information and how information should be destroyed. ITRC strongly recommends a breach notification similar to California's or New Jersey's current laws.

SSN as an identifier for customers or employees

In order to limit access of an individual's SSN, all companies should assign a separate account number and the SSN should never been seen on a call center screen by an employee of the company. There are many other ways, including passwords, to verify a person's identity.

Document Disposal

Finding: A popular spot identified by law enforcement and other investigative entities is the unshredded documents and data recklessly discarded into or near trash cans and dumpsters. Only several states have passed mandatory document disposal laws stating that paper and electronic documents must be rendered unreadable prior to disposal.

Example: A recent situation occurred in Los Angeles when the Department of Social Services had boxes of medical records, application forms and other documents with SSN put in boxes by a trash can. These documents never had been shredded but were being sent whole to China for recycling. Unfortunately they were also seen blowing in the wind and people went through boxes for information knowing they were out there.

Recommendation: A law that states that all documents, no matter what form they are in, must be rendered unreadable prior to leaving the entity that no longer wishes to store them.

Educational Facilities and SAT testing

Finding: In 2005 more than half of the disclosed breaches were educational facilities, mainly colleges and universities. The University of Colorado had 4 breaches in the last 14 months. After speaking with IT departments and administrators at several of these colleges, it is clear that changes need to be made. Parents send children to colleges to help them on their career paths. One identity theft problem can stop a future before it begins.

Recommendations: First, SSN should never be a student's public identification number, computer access number or publicly used for any other purpose. These steps will significantly limit the number of professors who have lost or had laptops stolen with student numbers and stop roster with names and SSNs from circulating classrooms.

Second, other than a few departments that are involved in payroll, student loans, scholarships and such should have access to the student's SSN. While it is easy to track a student by SSN it is easy to have that information securely stored in a database with limited access so that when a student asks for a transcript or school records they be found. However, the SSN should never be printed in full on any document sent through the mail.

Third, the "College Boards," the company that does SAT testing must immediately stop asking students for SSN and stop placing them on mailing labels. ITRC has had numerous calls about this activity.

Immigrants who no longer need or wish to have a SSN

Finding: ITRC has heard from a number of people who lived in the United States for a limited period of time or have moved from the United States to live permanently in another country. They would like a way to prevent any possible use of their SSN now that they no longer need it.

Recommendation: The creation of a national credit freeze program would not only help victims of identity theft and businesses from giving cards to thieves but would also solve this problem. However, that only solves the financial side of the problem. Other solutions would have to be found within the SSA so that those numbers would be tagged as inactive for employment or benefit purposes.

SSN of the Deceased

Finding: According to the SSA not all deceased individuals are on the Master Death Registry. It is partially consumer driven (change in benefit status) and partially populated by some states that do report all deaths to the SSA.

Recommendation: All governmental agencies that issue a death certificate should report that death to the SSA either directly or via a state program. Since this Registry is available to the credit reporting agencies and Department of Motor Vehicles this would significantly stop the use of a dead 7 year old's SSN by an adult.

SSNs sent through the mail

Finding: ITRC receives numerous inquiries from parents who never receive their newborns Social Security cards. Either they have been lost or intercepted by a would-be identity thief.

Recommendation: After talking with the Chief Privacy Officer of the U.S. Postal Service, there are a number of ways that the Post Office and SSA can work together to help insure the delivery of these documents. ITRC recommends that a committee be formed and a new procedure implemented within six months.

Finding: Companies still send information via the U.S. Mail with SSNs on mailing labels or in the body of the letter. In some cases it would clear to an identity thief that this envelope contains valuable information.

Recommendation: That mailing labels may never include a SSN and that when a SSN is included in the body of a document that it must be partially truncated.

IRS and selling of information

ITRC would be remiss if it did not comment on the plan being considered by the IRS to allow the sale by tax preparation services of our tax returns or personal tax information. Many people get numerous papers from tax preparers and just sign them. They go unread or may be beyond an individual's reading ability. This proposed plan must not be implemented. It creates another public record that will benefit thieves more than anyone else. If this must be allowed then there can be no allowances for acceptance of any release that is not clear and specific.

Public Records

Recommendation: The SSN should never be published on the Internet by a business or governmental entity including court records. In response to those who state they need that information, it can be specifically requested of the court, with appropriate redaction of unnecessary information that may place the individual in harm's way. This includes witness and victim information, family records during custody and divorce hearings and bankruptcy hearings.

Recommendation: In a court proceeding where information must be exchanged between opposing sides, the SSN should be at least partially redacted in order to protect the sanctity of that number.

New Laws—A Standard and not the Ceiling

The concepts discussed above are intended to benefit business and consumers. While we understand that companies don't want to deal with 50 different laws, it is also important to note that some states want to hold state and local governmental agencies and businesses to a higher standard than the ones recommended above. Any federal law should be a standard, to cover those citizens in states currently without information protection statutes and not pre-empt stronger state laws.

In Conclusion:

Protecting Social Security numbers from identity thieves needs to be everyone's job—not just the consumers. We need businesses and governmental agencies to work cooperatively with consumers to keep this valuable number out of the hands of those who have no regard for the damage they cause individuals and companies.

Businesses cannot afford to continue to lose money to identity thieves. While the numbers discussed in terms of fraud loss may sound like a trickle now, it is going to worsen. Identity thieves are more sophisticated, meth addicts have turned to this crime for money for fixes, and information trafficking is big business. Without required control procedures for the handling of Social Security numbers, this crime will worsen and our economy will suffer.

Its going to require the reeducation of consumers, businesses and governmental agencies. It going to require new behavior patterns, new ways of controlling information in the workplace and strict vigilance against new trends and attacks.

The proactive and not reactive protection of the Social Security number is in your hands. This small nine-digit number has the ability to destroy a company or an individual when misused. It is clear that some states have taken great strides to protect consumers. Unfortunately some business groups believe that anything that will benefit consumers will harm them and have fought change. Consumers blame businesses.

This is not a time for finger pointing. The blame game must end. We must be on the same team fighting a battle against this Goliath if we are to win. We must realize that we are one people and anything that harms one of us harms us all.

Thank you for your time and interest.

Linda Foley

Jay Foley

Chairman MCCRERY. Thank you, Ms. Robinson. Ms. McQueen?

STATEMENT OF MARY C. McQUEEN, PRESIDENT, NATIONAL CENTER FOR STATE COURTS, ON BEHALF OF THE CONFERENCE OF STATE COURT ADMINISTRATORS

Ms. MCQUEEN. Thank you, Mr. Chairman, Mr. Levin, Members of the Subcommittee. I am Mary McQueen. The Conference of State Court Administrators is pleased to present testimony on today's hearings before this important Committee.

Before I begin my remarks, I would like to provide some background about who that group is, and I submit testimony on their behalf. I am a former member of the Conference of State Court Administrators, having served as the Chief Administrative Officer for the court system in the State of Washington for 25 years, and most recently assumed the position as the President for the National Center for State Courts. The National Center operates in coordina-

tion with the Conference of State Court Administrators and Chief Justices in a similar way that the Federal Judicial Center operates with the Federal judiciary.

The Conference of State Court Administrators and the Conference of Chief Justices represent the top judicial officials and chief administrative officers in the 58 States, Commonwealths, and U.S. Territories, and we work very closely together with the chief justices to develop best practices to improve the administration of justice. You may know that more than 98 percent of all judicial proceedings in the United States are in State courts that consist of over 30,000 judges and over 16,000 courts.

Mr. Chairman, let me begin by informing you that the State courts have taken several important steps to protect individual privacy and we share the Committee's concerns. The State courts hope to partner with the Chair and the Members of this Subcommittee in your efforts to increase those privacy steps.

A question we are always asked is why do State courts need SSNs? What is the State courts' interest in collecting those numbers, and why do State courts require parties to provide them in litigation? I would like to just briefly identify five different uses of the SSN in State courts.

The first and obvious one to those of you who are members of the bar is to ensure that accurate information is placed before a fact finder. We want to ensure, especially in family law cases, that we have access to the information that is necessary to determine child support, to distribute property, and to determine paternity.

Secondly, we also need to identify the parties. Courts often use SSNs to identify criminal defendants that lack fingerprint information.

We also use SSNs to enforce judgments in court orders. Courts often order restitution or the repayment of fines as a legal judgment, and SSNs have become the universal commercial identifier for use in monetary penalties. Litigants' SSNs are also necessary for use in State income tax intercept programs, where outstanding monetary judgments are deducted from State income tax returns. Federal law now requires State courts to place a party's SSN in records relating to divorce and child support decrees, and in October 1999, that requirement was extended to require SSNs for all children to whom support is required to be paid.

We also need SSNs to create jury pools and to pay jurors. It requires us when we issue a check to jurors that that income is reported, and we are required to have SSNs for those individuals.

Finally, we use SSNs to notify the SSA of incarcerated and absconded persons. The SSA cuts off payments to persons incarcerated in all Federal, State, and local prisons or jails who are fugitives from justice and they need to identify those persons. While traditionally that information comes from correctional agencies, the courts initially provide those agencies with that information.

As previously mentioned, the Welfare Reform Act (P.L. 104-193) does require courts to collect SSNs on court orders granting divorces, providing for child support, or determining paternity, and SSNs can appear in many financial records, such as tax returns, which are required to be filed in many court proceedings.

We were encouraged by some of the language that accompanied H.R. 2971 in the report dealing with incidental versus non-incidental appearances of SSNs on public records and we would encourage that if you move forward, we would like to work with you on looking at some of those provisions.

In drafting Social Security legislation, we respectfully request that you ask members of the court community participate in those discussions.

Finally, in an effort to increase privacy and reduce the possibility of identity theft from court documents, the chief justices and the State court administrators have established a Standing Committee on Court Privacy and Access to Court Records. They have adopted national guidelines and model court rules, and we have identified three best practices. I would draw your attention to our visual aid here.

These best practices include creating basically two sets of records. The State of Washington, the States of Michigan, Vermont, and South Dakota have adopted this approach, where basically in the types of records that incorporate sensitive information as well as SSN, there is a special procedure for sealing this information, placing them in a separate file, and when someone comes to the counter and asks to see the court file, those records are removed in the envelope and not provided to the public.

We have also identified a best practices that we give an alert to the filing parties and make sure that they know they are responsible for including any SSNs in the documents that are filed and make sure that on all court model forms, that everybody uses, that there is an alert saying your SSN may be available, so please consider not including that.

Also, as part of the two sets of records, several States have identified confidentiality filing forms, where you put that information on one sheet, not incorporate it into the court documents, and that one sheet is sealed.

Finally, when requiring SSNs, we have recommended that you only use four digits that would appear in the court record.

Mr. Chairman, we recognize the threat of identity theft as real. We commit that the State courts want to do our part in eliminating that opportunity. I have presented several reasons why the courts utilize SSNs as well as the solutions that we are working to implement.

Thank you for allowing us to participate in this discussion and I will be happy to answer any questions you may have.

[The prepared statement of Ms. McQueen follows:]

Statement of Mary C. McQueen, on behalf of the Council of State Court Administrators, Williamsburg, Virginia

Mr. Chairman and Members of the Subcommittee,

The Conference of State Court Administrators (COSCA) is pleased to present testimony on today's fifth in a series of hearings on Social Security Number High Risk Issues.

SUMMARY

Mr. Chairman and members of the subcommittee, the state court community has been grappling with the issue of protecting privacy as it relates to court records for the past few years. We are taking a proactive stance in protecting the privacy of individuals and their social security numbers, while at the same time maintaining

traditional open court access. Today, we will share examples of what state courts that are doing on this via the approval of court rules.

In collaboration with the Conference of Chief Justices (CCJ), we established a project entitled "Public Access to Court Records: CCJ/COSCA Guidelines for Policy Development by State Courts," which outlines the issues that a jurisdiction must address in developing its own rules, and provides one approach. The *Guidelines* touch on the use of social security numbers (SSNs) in court records as well as other private information. The entire text of the *Guidelines* can be found online at <http://www.courtaccess.org/modelpolicy/18Oct2002FinalReport.pdf>. Both CCJ and COSCA, adopted a resolution endorsing the *Guidelines* and urged the states to address them.

Mr. Chairman, SSNs are pervasive in state court documents and procedures. The testimony that follows gives the subcommittee numerous examples of how we use SSNs in day-to-day court proceedings. For example, we use SSNs to insure that judges have the best evidence available to them. We also use SSNs to collect fines and restitution. In addition, many SSNs appear in the public record in many types of court cases including, but not limited to, bankruptcy, divorce and child support cases. My testimony also details the federal requirements imposed on us to collect SSNs for various reasons, for example, to track parents who are not paying child support.

Mr. Chairman, we stand ready to work with you to craft solutions to address the problem of identity theft. We want to do our part to eliminate it. We are at the same time concerned about the effort to require us to redact or expunge SSNs that appear in public records. We feel that this type of requirement would impose an unfunded mandate on state courts in this country. The cost to fulfill this requirement would be high because many SSNs appear in paper documents as well as other hard-to-redact microfilm/microfiche.

ABOUT COSCA

Before I begin my remarks, I would like to provide some background on our group and our membership. I submit this testimony on behalf of the Conference of State Court Administrators (COSCA). I am a former member of COSCA having served as State Court Administrator of the state of Washington. The National Center for State Courts, of which I am President, serves as secretariat to COSCA. COSCA was organized in 1955 and is dedicated to the improvement of state court systems. Its membership consists of the principal court administrative officer in each of the fifty states, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and the Territories of American Samoa, Guam, and the Virgin Islands. A state court administrator implements policy and programs for a statewide judicial system. COSCA is a nonprofit corporation endeavoring to increase the efficiency and fairness of the nation's state court systems. As you know, state courts handle 98% of all judicial proceedings in the country. The purposes of COSCA are:

- To encourage the formulation of fundamental policies, principles, and standards for state court administration;
- To facilitate cooperation, consultation, and exchange of information by and among national, state, and local offices and organizations directly concerned with court administration;
- To foster the utilization of the principles and techniques of modern management in the field of judicial administration; and
- To improve administrative practices and procedures and to increase the efficiency and effectiveness of all courts.

Although I do not speak for them today, I also would like to tell you about the Conference of Chief Justices (CCJ), a national organization that represents the top judicial officers of the 58 states, commonwealths, and U.S. territories. Founded in 1949, CCJ is the primary voice for state courts before the federal legislative and executive branches and works to promote current legal reforms and improvements in state court administration. COSCA works very closely with CCJ on policy development and administration of justice issues.

STATE COURTS ARE RESPONDING TO PRIVACY CONCERNS

Mr. Chairman, let me begin by informing you of the progress that many state courts are making to protect individual privacy rights, while maintaining the American tradition of open courts. Through court rules, state court systems are changing their procedures for viewing and accessing court records as they relate to the appearance of social security numbers. Washington State, for example, is establishing a procedure for "sealing" family case court records containing privileged information such as social security numbers and financial information. In effect, Washington is

creating two sets of records: a public and a private one. Vermont is placing the burden on parties to expunge or redact social security numbers from papers filed with the court. Minnesota is requiring that parties in a divorce case fill out a confidential information sheet, which contains social security numbers, to be kept separate from the official record. South Dakota adopted a rule that protects SSNs and financial account number information by requiring these numbers to be redacted from documents and submitted to the Court on confidential information forms. As an example, I am attaching the South Dakota rule along with their required confidential information sheet to the end of my testimony.

In addition to the proactive stance we are taking to this issue, we are also responding to some of the demands placed on our court systems by state legislatures and governors. In 2005, 53 bills were signed into law by governors dealing with social security number privacy. That's 17 more than in 2004; an increase of 46 percent. These bills range from simple prohibition of displays of SSNs on public records to new expansive criminal and civil statutes that punish wrongdoers and those that traffic in social security numbers as a means to steal a person's identity. Activity in this area has not diminished in the current year. In the ongoing 2006 sessions, state legislatures are considering 176 measures dealing with social security numbers and privacy. Again, this number is an increase over the prior year.

At the direction of the CCJ and COSCA leadership, we established a special subcommittee of the CCJ/COSCA Court Management Committee to explore privacy protection innovations and share them with the Congress and the Administration. This committee meets twice a year at our annual and mid-year meetings. This subcommittee has been researching the issue and is responsible for compiling examples of best practices in this area that I am presenting today.

NATIONAL EFFORT TO CRAFT PUBLIC ACCESS GUIDELINES TO COURT RECORDS

Our project entitled, "Public Access to Court Records: CCJ/COSCA Guidelines for Policy Development by State Courts" was a joint effort of CCJ/COSCA and the NCSC to give state court systems and local trial courts assistance in establishing policies and procedures that balance the concerns of personal privacy, public access and public safety.

The State Justice Institute (SJI) funded this project in 2001 and it was staffed by the NCSC and the Justice Management Institute. The project received testimony, guidance and comments from a broad-based national committee that included representatives from courts (judges, court administrators, and clerks), law enforcement, privacy advocates, the media, and secondary users of court information.

The *Guidelines* recommend the issues that a jurisdiction must address in developing its own rules governing public access. The *Guidelines* are based on the following premises:

- Retention of the traditional policy that court records are presumptively open to public access
- The criteria for access should be the same regardless of the form of the record (paper or electronic), although the manner of access may vary
- The nature of certain information in some court records is such that remote public access to the information in electronic form may be inappropriate, even though public access at the courthouse is maintained
- The nature of the information in some records is such that all public access to the information should be precluded, unless authorized by a judge
- Access policies should be clear, consistently applied, and not subject to interpretation by individual courts or court personnel

The *Guidelines* Committee examined the use of SSNs in current court practices. They looked at the inclusion of SSNs in bulk distribution of court records, and in other private information that courts traditionally protect, such as addresses, phone numbers, photographs, medical records, family law proceedings, and financial account numbers. Finally, the Committee examined various federal laws and requirements governing SSN display and distribution by state and local entities.

On August 1, 2002, CCJ and COSCA endorsed and commended "the *Guidelines* to each state as a starting point and means to assist local officials as they develop policies and procedures for their own jurisdictions."

STATE COURTS' INTEREST IN COLLECTING AND USING SOCIAL SECURITY NUMBERS

A question we are often asked is why do state courts utilize SSNs? What is the state court interest in collecting SSNs? Why do state courts need to require parties

to provide their SSNs in the course of state court litigation? The following are some of the reasons we use them:

Accurate determination of assets/income Judges need the most accurate information on assets and income when making their decisions, especially in family law cases. In many instances this involves examining assets by a social security number. There are numerous examples of individuals giving a false social security number to avoid paying child support, for example. The same logic applies in dealing with divorce cases in dividing assets.

Identification of parties A growing number of court systems are using case management information systems in which an individual's name, address, and telephone number are entered once, regardless of the number of cases in which the person is a party. The advantage of these systems is to be able to update an address or telephone number for all cases in which the person is a party by a single computer entry. SSNs provide a unique identifier by which court personnel can determine whether the current "John Smith" is the same person as a previous "John Smith" who appeared in an earlier case.

Courts have often used SSNs to identify criminal defendants as well as parties to civil cases. In the future, persons accused of crime will be identified by automated fingerprint identification systems (AFIS) which scan fingerprints and classify them electronically. The primary future need for SSNs as a means to identify individuals will therefore be in civil, not criminal, litigation.

Collection of fees, fines and restitution by courts SSNs are the universal personal identifier for credit references, tax collection, and commercial transactions.

When courts give a litigant an opportunity to pay an assessment resulting from a judgment in periodic payments, the court needs to be able to function as a collection agency. Having the convicted person's social security number is necessary for use of state tax intercept programs (in which a debt to the state is deducted from a taxpayer's state income tax refund) and other collection activities. Some states use additional means to enforce criminal fines and restitution orders, such as denial of motor vehicle registration; SSNs are often used for these purposes as well.

Creation of jury pools and payment of jurors SSNs are a necessary part of the process by which multiple lists (for instance, registered voters and registered drivers) are merged by computer programs to eliminate duplicate records for individual citizens in the creation of master source lists from which citizens are selected at random for jury duty. Duplicate records double an individual's chance of being called for jury duty and reduce the representativeness of jury panels. Some courts use SSNs to pay jurors as well.

Making payments to vendors SSNs are used as vendor identification numbers to keep track of individuals providing services to courts and to report their income to state and federal taxing authorities.

Facilitating the collection of judgments by creditors and government agencies Courts are not the only entities that need to collect judgements. Judgment creditors need SSNs to locate a judgment debtor's assets and levy upon them. Courts often require that the judgment debtor make this information available without requiring separate discovery proceedings that lengthen the collection process and increase its costs. Federal law now requires state courts to place the parties' SSNs in the records relating to divorce decrees, child support orders, and paternity determinations or acknowledgements in order to facilitate the collection of child support. On October 1, 1999, that requirement was extended to include the SSNs of all children to whom support is required to be paid.

Notification to the Social Security Administration of the names of incarcerated and absconded persons The Social Security Administration cuts off all payments to persons incarcerated in federal, state or local prison or jails, and to persons who are currently fugitives from justice. The savings to the federal budget from this provision are substantial. To implement this process, Social Security Administration needs to identify persons who have been sentenced to jail or prison and persons for whom warrants have been issued. The agency has traditionally obtained this information from state and local correctional agencies. See 42 USC § 402(x)(3) requiring Federal and State agencies to provide names and SSNs of confined persons to the Social Security Administration. The state courts of Maryland are involved in an experimental program to provide such information directly from court records. The Maryland program has two additional future advantages for state courts. First, the program offers the possibility of obtaining better addresses for many court records; social security and other welfare agencies have the very best address records because of beneficiaries' obvious interest in maintaining their currency. Second, cutting off benefits may provide a useful incentive for persons receiving benefits to clear up outstanding warrants without requiring the expenditure of law enforcement resources to serve them.

Transmitting information to other agencies In addition to the Social Security Administration, many states provide information from court records to other state agencies. A frequently occurring example is the Motor Vehicle Department, to which courts send records of traffic violations for enforcement of administrative driver's license revocation processes. These transfers of information often rely upon SSNs to ensure that new citations are entered into the correct driver record.

POTENTIAL LEGISLATION

Mr. Chairman, in the past, this subcommittee has considered various pieces of legislation that would, in some form or another, prohibit the display of a person's social security number on a public record. Blanket prohibitions like these will place courts in the position of trying to comply with conflicting public policies. We submit the following questions for your consideration:

The Welfare Reform Law requires courts to collect SSNs on court orders granting divorces or child support or determining paternity. State laws contain similar requirements in other types of cases in some states. What steps must a court take to restrict access to these documents, which are matters of public record in most states?

SSNs appear in many financial documents, such as tax returns, which are required to be filed in court (e.g., for child support determinations) or are appended to official court documents, such as motions for summary judgments. What steps must a court take to restrict access to these documents, which are also matters of public record in most states?

We were encouraged by language in the report accompanying HR 2971 (Rept. 108-685, Part 1, p. 21) in the 108th Congress dealing with incidental vs. non-incidental appearances of SSNs in public records:

During Social Security Subcommittee hearings on the bill, court and other public records administrators testified they receive numerous documents filed by individuals, businesses, and attorneys that often include SSNs the government did not require to be submitted, and of which they are therefore unaware. They stated redaction of "incidentally" included SSNs would create a serious administrative burden, and it would require significant resources to review each document and redact such incidental SSNs—*With respect to SSNs submitted in court documents absent the court's requirement to do so, the individual communicating the SSN in the document, not the court, would be held responsible according to Section 108 of the bill.* (Emphasis ours)

In drafting social security legislation, we respectfully ask that you expand on the above sentiments in actual legislative language of any future bill.

Courts will have substantial increased labor costs in staff time to redact or strike the appearance of SSNs in paper records or in microfilm/microfiche if a redaction requirement is imposed.

In the event you draft legislation dealing with redaction, we urge you to make a distinction between existing court records/documents and future documents. For example, requiring a court to retroactively redact or expunge old records would be a nightmarish task due to the cost in staff time and the actual compiling of said court records.

Finally, in an effort to make courts and court records more open, many courts are now beginning to make available many public records on the internet either as text/character documents or by scanning and placing them online through imaging software (PDF files). While the removal of SSNs in text/character documents may be relatively easy in some computer generated records (XML), other scanned records, such as PDF files, will be harder to change necessitating more staff and an increase in labor costs.

OUR FUTURE COURSE OF ACTION

CCJ and COSCA have recommended that state courts adopt the following policies, unless state law directs them otherwise, to protect citizen privacy while providing service to litigants:

Official court files State courts should not attempt to expunge or redact SSNs that appear in documents that are public records. As was mentioned earlier, federal law requires state courts to place the parties' SSNs in the records relating to divorce decrees, child support orders, and paternity determinations or acknowledgement in order to facilitate the collection of child support. The purpose of placing that data on judgments is not just to provide it to child support enforcement agencies; it is also to provide it to the parties themselves for their own private enforcement efforts. Any other interpretation puts the courts in an untenable position—having an affirmative obligation to provide judgments in one form to parties and child support enforcement agencies and in another form to all other persons.

This same reasoning applies to income tax returns or other documents containing SSNs filed in court. It would be unreasonable, and expensive, to expect courts to search every document filed for the existence of SSNs. Further, court staff has no authority altering documents filed in a case; the social security number may have evidentiary value in the case—at the very least to confirm the identity of the purported income tax filer.

Case management information databases Data in automated information systems raises more privacy concerns than information in paper files. Automated data can be gathered quickly and in bulk, can be manipulated easily, and can be correlated easily with other personal data in electronic form. Data in an automated database can also be protected more easily from unauthorized access than data in paper files. It is feasible to restrict access to individual fields in a database altogether or to limit access to specific persons or to specific categories of persons. Consequently, state courts should take steps to restrict access to SSNs appearing in court databases. They should not be available to public inquirers. Access to them should be restricted to court staff and to other specifically authorized persons (such as child support enforcement agencies) for whose use the information has been gathered.

Staff response to queries from the public When court automated records include SSNs for purposes of identifying parties, court staff should be trained not to provide those numbers to persons who inquire at the public counter or by telephone. However, staff may confirm that the party to a case is the person with a particular social security number when the inquirer already has the social security number and provides it to the court staff member.

In short, staff may not read aloud a social security number, but may listen to a social security number and confirm that the party in the court's records is the person with that number. This is the same distinction applied to automated data base searches. This distinction is one commonly followed in federal and state courts.

CONCLUSION

Mr. Chairman, we recognize the role of SSNs in the incidence of identity theft cases. The current state of affairs with regards to the treatment of SSNs provides lawbreakers the continued opportunity to exploit the current system at the expense of ordinary Americans. The threat of identity theft is real and we want to do our part to eliminate it.

I have presented several ways our courts utilize SSNs. Finding solutions to protect an individual's privacy will be complex and difficult. Many state courts are already taking steps to fashion solutions in response to the problem. I remind you of the earlier mentioned approaches from Washington, Vermont, Minnesota and South Dakota. Other states are experimenting with different approaches.

Thank you for asking for our input on this important matter. The Conference of State Court Administrators stands ready to work collaboratively and cooperatively to craft solutions to this important issue. I will be happy to answer any questions you may have.

Example of South Dakota court rule to protect SSNs from public dissemination

UNIFIED JUDICIAL SYSTEM

COURT RECORDS rule

SDCL ch. 15-15A

SDCL 15-15A-1. Purpose of rule of access to court records.

The purpose of this rule is to provide a comprehensive policy on access to court records. The rule provides for access in a manner that:

- (1) Maximizes accessibility to court records,
- (2) Supports the role of the judiciary,
- (3) Promotes governmental accountability,
- (4) Contributes to public safety,
- (5) Minimizes risk of injury to individuals,
- (6) Protects individual privacy rights and interests,
- (7) Protects proprietary business information,
- (8) Minimizes reluctance to use the court to resolve disputes,
- (9) Makes most effective use of court and clerk of court staff,
- (10) Provides excellent customer service, and
- (11) Does not unduly burden the ongoing business of the judiciary.

The rule is intended to provide guidance to 1) litigants, 2) those seeking access to court records, and 3) judges, court and clerk of court personnel responding to requests for access.

SDCL 15-15A-2. Eho has access to court records under the rule.

Every member of the public has the same access to court records as provided in this rule, except as provided otherwise by statute or rule and except as provided in § 15-15A-7.

"Public" includes:

- (1) any person and any business or non-profit entity, organization or association;
- (2) any governmental agency for which there is no existing policy, statute or rule defining the agency's access to court records;

(3) media organizations.

"Public" does not include:

- (4) court or clerk of court employees;
- (5) people or entities, private or governmental, who assist the court in providing court services;

(6) public agencies whose access to court records is defined by another statute, rule, order, policy or database access agreement with the South Dakota Unified Judicial System;

(7) the parties to a case or their lawyers regarding access to the court record in their case, which may be defined by statute or rule.

SDCL 15-15A-3. Definition of terms.

(1) "Court record" includes any document, information, or other thing that is collected, received or maintained by a clerk of court in connection with a judicial proceeding. "Court record" does not include other records maintained by the public official who also serves as clerk of court or information gathered, maintained or stored by a governmental agency or other entity to which the court has access but which is not part of the court record as defined in this section.

(2) Information in a court record "in electronic form" includes information that exists as: (a) electronic representations of text or graphic documents; (b) an electronic image, including a video image, of a document, exhibit or other thing; or (c) data in the fields or files of an electronic database.

(3) "Public access" means that the public may inspect and obtain a copy of the information in a court record unless otherwise prohibited by statute, court rule or a decision by a court of competent jurisdiction. The public may have access to inspect information in a court file upon payment of applicable fees.

(4) "Remote access" means the ability to electronically search, inspect, or copy information in a court record without the need to physically visit the court facility where the court record is maintained.

SDCL 15-15A-4. Applicability of rule.

This rule applies to all court records, regardless of the physical form of the court record, the method of recording the information in the court record or the method of storage of the information in the court record.

SDCL 15-15A-5. General access rule.

(1) Information in the court record is accessible to the public except and as prohibited by statute or rule and except as restricted by §§ 15-15A-7 through 15-15A-13.

(2) There shall be a publicly accessible indication of the existence of information in a court record to which access has been restricted, which indication shall not disclose the nature of the information protected, i.e., "sealed document."

(3) An individual circuit or a local court may not adopt a more restrictive access policy or otherwise restrict access beyond that provided by statute or in this rule, nor provide greater access than that provided for by statute or in this rule.

SDCL 15-15A-6. Court records that are only publicly available at a court facility.

A request to limit public access to information in a court record to a court facility in the jurisdiction may be made by any party to a case, an individual identified in the court record, or on the court's own motion. For good cause, the court will limit the manner of public access. In limiting the manner of access, the court will use the least restrictive means that achieves the purposes of this access rule and the needs of the requestor.

SDCL 15-15A-7. Court records excluded from public access.

The following information in a court record is not accessible to the public:

- (1) Information that is not to be accessible to the public pursuant to federal law;
- (2) Information that is not to be accessible to the public pursuant to state law, court rule or case law as follows;

(3) Examples of such state laws, court rules, or case law follow. Note this may not be a complete listing and the public and court staff are directed to consult state

law, court rules or case law. Note also that additional documents are listed below that may not be within court records but are related to the court system; the public and court staff should be aware of access rules relating to these documents.

- (a) Abortion records (closed); § 34-23A-7.1
- (b) Abuse and neglect files and records (closed, with statutory exceptions); § 26-8A-13
- (c) Adoption files and adoption court records (closed, with statutory exceptions); §§ 25-6-15 through 25-6-15.3
- (d) Affidavit filed in support of search warrant (sealed if so ordered by court, see statutory directives); § 23A-35-4.1
- (e) Attorney discipline records (closed until formal complaint has been filed with Supreme Court by the State Bar Association's Disciplinary Board or Attorney General, accused attorney requests matter be public, or investigation is premised on accused attorney's conviction of a crime); § 16-19-99
- (f) Civil case filing statements (closed); § 15-6-5(h)
- (g) Coroner's inquest (closed until after arrest directed if inquisition finds criminal involvement with death); § 23-14-12
- (h) Custody or visitation dispute mediation proceedings pursuant to § 25-4-60 (closed, inadmissible into evidence)
- (i) Discovery material (closed unless admitted into evidence by court) §§ 15-6-26(c); 15-6-5(g)
- (j) Domestic abuse victim's location (closed, with statutory exception); § 25-10-39
- (k) Employment examination or performance appraisal records maintained by Bureau of Personnel (closed); § 1-27-1
- (l) Grand jury proceedings (closed with statutory exceptions); § 23A-5-16
- (m) Guardianships and conservatorships (closed with statutory exceptions); § 29A-5-311
- (n) Involuntary commitment for alcohol and drug abuse (petition, application, report to circuit court and court's protective custody order sealed; law enforcement or prosecutor may petition the court to examine these documents for limited purpose); § 34-20A-70.2
- (o) Judicial disciplinary proceedings (closed until Judicial Qualifications Commission files its recommendation to Supreme Court, accused judge requests matter be public, or investigation is premised on accused judge's conviction of either a felony crime or one involving moral turpitude); ch. 16-1A, Appx. III(1)
- (p) Juvenile court records and court proceedings (closed with statutory exception); § 26-7A-36 through -38; §§ 26-7A-113 through -116
- (q) Mental illness court proceedings and court records (closed); §§ 27A-12-25; 27A-12-25.1 through -32
- (r) Pardons (statutory exceptions, see § 24-14-11)
- (s) Presentence investigation reports (closed); §§ 23A-27-5 through -10; § 23A-27-47
- (t) Probationer under suspended imposition of sentence (record sealed upon successful completion of probation conditions and discharge); §§ 23A-27-13.1; 23A-27-17
- (u) Records prepared or maintained by court services officer (closed except by specific order of court); § 23A-27-47
- (v) Trade secrets (closed); § 15-6-26(c)(7)
- (w) Trusts (sealed upon petition with statutory exceptions); § 21-22-28
- (x) Voluntary termination of parental rights proceedings and records (closed except by order of court); § 25-5A-20
- (y) Wills (closed with statutory exceptions); § 29A-2-515
- (z) Written communication between attorney and client; attorney work product (closed unless such privilege is waived); ch. 16-18, Appx. Rule 1.6
- (aa) Information filed with the court pending in camera review (closed)
- (bb) Any other record declared to be confidential by law; § 1-27-3.

SDCL 15-15A-8. Confidential numbers and financial documents excluded from public access.

The following information in a court record is not accessible to the public.

- (1) Social security numbers, employer or taxpayer identification numbers, and financial account numbers of a party or party's child.
- (2) Financial documents such as income tax returns, W-2's and schedules, wage stubs, credit card statements, financial institution statements, credit card account statements, check registers, and other financial information.

SDCL 15-15A-9. Filing confidential numbers and financial documents in court records.

(1) Social security numbers, employer or taxpayer identification numbers, and financial account numbers of a party or party's child, where required to be filed with the court shall be submitted on a separate Confidential Information Form, appended to these rules, and filed with the pleading or other document required to be filed. The Confidential Information Form is not accessible to the public.

(2) Financial documents named in § 15-15A-8(2) that are required to be filed with the court shall be submitted as a sealed document and designated as such to the clerk upon filing. The Sealed Financial Documents Information Form appended to these rules shall be attached to financial documents being filed with the court. The Sealed Financial Documents Information Form is confidential and is not accessible to the public. The sealed financial documents will not be publicly accessible, even if admitted as a trial or hearing exhibit, unless the court permits access pursuant to § 15-15A-10. The court may, on its own motion, seal financial documents that have been submitted without the Sealed Financial Documents Information Form.

(3) Parties with cases filed prior to the effective date of this rule, or the court on its own, may, by motion, protect the privacy of confidential information as defined in § 15-15A-8. Parties filing this motion will submit a completed Confidential Information Form or Sealed Financial Documents Information Form as appropriate.

SDCL 15-15A-10. Procedure for requesting access to sealed financial documents.

(1) Any person may file a motion, supported by affidavit showing good cause, for access to sealed financial documents. Written notice of the motion shall be required.

(2) If the person seeking access cannot locate a party to provide the notice required under this rule, after making good faith reasonable effort to provide such notice as required by applicable court rules, an affidavit may be filed with the court setting forth the efforts to locate the party and requesting waiver of the notice provisions of this rule. The court may waive the notice requirement of this rule if the court finds that further good faith efforts to locate the party are not likely to be successful.

(3) The court shall allow access to sealed financial documents, or relevant portions of the documents, if the court finds that the public interest in granting access or the personal interest of the person seeking access outweighs the privacy interests of the parties or dependent children. In granting access the court may impose conditions necessary to balance the interests consistent with this rule.

SDCL 15-15A-11. Requests for bulk distribution of court records.

Dissemination of bulk information for resale is prohibited pursuant to § 1-27-1. Any other bulk dissemination is prohibited except as authorized by the State Court Administrator or the Chief Justice of the Supreme Court.

SDCL 15-15A-12. Access to compiled information from court records.

(1) Compiled information is defined as information that is derived from the selection, aggregation or reformulation by the Supreme Court of some of the information from more than one individual court record.

(2) Any member of the public may request compiled information that consists solely of information that is publicly accessible and that is not already available in an existing report. The Supreme Court may compile and provide the information if it determines, in its discretion, that providing the information meets criteria established by the Court, that the resources are available to compile the information and that it is an appropriate use of public resources. The State Court Administrator's Office will make the initial determination as to whether to provide the compiled information.

(a) Compiled information that includes information to which public access has been restricted may be requested by any member of the public only for scholarly, journalistic, political, governmental, research, evaluation, or statistical purposes.

(b) The request shall a) identify what information is sought; b) describe the purpose for requesting the information and explain how the information will benefit the public interest or public education, and c) explain provisions for the secure protection of any information requested to which public access is restricted or prohibited.

(c) The Supreme Court may grant the request and compile the information if it determines that doing so meets criteria established by the Court, is consistent with the purposes of the access rules, that the resources are available to compile the information, and that it is an appropriate use of public resources.

(d) If the request is granted, the Supreme Court may require the requestor to sign a declaration that:

(i) The data will not be sold or otherwise distributed directly or indirectly, to third parties, except for journalistic purposes;

(ii) The information will not be used directly or indirectly to sell a product or service to an individual or the general public, except for journalistic purposes; and

(iii) There will be no copying or duplication of information or data provided other than for the stated scholarly, journalistic, political, governmental, research, evaluation, or statistical purpose.

The Supreme Court may make such additional orders as may be needed to protect information to which access has been restricted or prohibited.

SDCL 15-15A-13. Requests to prohibit public access to information in court records.

A request to prohibit public access to information in a court record may be made by any party to a case, the individual about whom information is present in the court record, or on the court's own motion. Notice of the request must be provided to all parties in the case and the court may order notice be provided to others with an interest in the matter. The court shall hear any objections from other interested parties to the request to prohibit public access to information in the court record. The court must decide whether there are sufficient grounds to prohibit access according to applicable constitutional, statutory and common law. In deciding this the court should consider the purpose of this rule as set forth in § 15-15A-1. In restricting access, the court will use the least restrictive means that will achieve the purposes of this access rule and the needs of the requestor.

SDCL 15-15A-14. When court records may be accessed.

(1) Court records will be available where available for public access in the courthouse during hours established by the court. Court records in electronic form to which the court allows remote access under this rule will be available for access at least during the hours established by the court for courthouse access, subject to unexpected technical failures or normal system maintenance announced in advance.

(2) Upon receiving a request for access to information the court will respond within a reasonable time regarding the availability of the information and provide the information within a reasonable time.

SDCL 15-15A-15. Fees for accessing court records.

The Supreme Court may charge a fee for access to and copies of court records in electronic form, for remote access or compiled information. The fee shall be reasonable and may include costs for labor, materials and supplies. Fees for record searches are set forth in § 16-2-29.5. Some entities, and other entities under certain conditions, are exempt from paying a record search fee pursuant to § 16-2-29. Copying and certification fees shall be charged as determined by statute or Supreme Court Rule.

CONFIDENTIAL INFORMATION FORM (Required by SDCL 15-15A-9)

Case No. _____
Plaintiff/Petitioner _____

Defendant/Respondent _____

The information on this form is confidential and shall not be placed in a publicly accessible portion of a court record.

NAME _____

SOCIAL SECURITY NUMBER _____

EMPLOYER IDENTIFICATION NUMBER _____

TAXPAYER IDENTIFICATION NUMBER _____

FINANCIAL ACCOUNT NUMBERS: _____

Plaintiff/Petitioner _____

1. _____

2. _____

3. _____

Defendant/Respondent _____

1. _____

2. _____

3. _____

Other Parties (including minor children) _____

1. _____

2. _____

3. _____

4. _____

Information supplied by: _____

Signed: _____

Firm: _____

Address: _____

Date: _____

SEALED FINANCIAL DOCUMENTS INFORMATION FORM (Required by
SDCL 15-15a-9)

_____ Case No. _____
Plaintiff/Petitioner

_____ Defendant/Respondent

**The information on this form is confidential and shall not be placed in a
publicly accessible portion of a court record.**

_____ Income Tax Records

Period Covered:

_____ Financial Account Statements

Period Covered:

_____ Wage Stubs

Period Covered:

_____ Credit Card Account Statements

Period Covered:

_____ Other

Information supplied by: _____

Signed: _____

Firm: _____

Address: _____

Date: _____

Chairman MCCRERY. Thank you, Ms. McQueen. Mr. Stein?

**STATEMENT OF ERIK STEIN, EXECUTIVE VICE PRESIDENT
AND DIRECTOR, FRAUD RISK MANAGEMENT, COUNTRYWIDE
FINANCIAL CORPORATION, ON BEHALF OF BITS FRAUD RE-
DUCTION STEERING COMMITTEE**

Mr. STEIN. Thank you. Good afternoon, Chairman McCrery and Members of the Subcommittee. My name is Erik Stein. I am Executive Vice President and Director of Fraud Risk Management at Countrywide, America's largest residential mortgage lender and servicer, currently responsible for preventing, detecting, investigating, mitigating, and reporting on criminal conduct by, through, or within Countrywide Financial Corporation and its member family of companies.

I am pleased to appear before you today on behalf of BITS and the Financial Services Roundtable to discuss the role of SSNs in identity theft and SSN privacy. I have submitted a more detailed written statement for the record, but would like to highlight five key points in my oral statement.

First, SSNs have evolved, regardless of their original intent, to become the de facto unique identifier that today accompanies most consumers from cradle to grave. SSNs provide the link to associate consumers to their financial accounts, credit reports, public records, and a host of other critical relationships. SSNs are essential to financial institutions to meet various statutory obligations, such as knowing their customers, report tax-related activity, conduct financial crimes investigations, screen prospective employees, and more. All of these functions help keep our customers and their financial assets safe and ensure the security and reliability of the economy.

Second, SSNs play a pivotal role in the accurate determination of an individual. With millions of citizens in America, the SSN is the single unique identifier common to them all. However, it is important to note that the verification of the SSN is not the same as the verification of identity. Verification of identity is accomplished through the use of other government-issued documentation, including drivers' licenses and passports, which financial institutions require to open accounts and make loans. However, financial institutions have not been afforded the tools to ensure the validity of SSNs and these other documents presented for identity verification even though the institutions are required by the USA PATRIOT Act (P.L. 107-56) to know their customers.

That brings me to my third point, which is the proposed consent-based SSN verification, or CBSV program recently established by

the SSA, is a critical first step in facilitating identity verification. The program allows verification of the SSN along with the corresponding name and date of birth provided by consumers to SSA's database. I and other fraud reduction professionals strongly encourage the Subcommittee to actively support the CBSV program and we urge the SSA to remove restrictions on the daily submission volume by participants, work to improve the proposed response times, eliminate the requirements for a stand-alone consumer authorization, allowing the authorization to be incorporated into loan or account documents, and review the cost structure. These changes would allow participants to consistently use CBSV on every new relationship, reducing fraud, identifying errors, and lowering costs.

Fourth, criminals know the intrinsic value of SSNs in committing identity theft and other crimes. The sad reality is that criminals in search of identities with which to commit identity theft can readily obtain them through many means. For example, all a criminal need do is steal mail in January, when millions of 1099s and 1098s are distributed to taxpayers. These forms are required by statute to display the SSN and for mailing purposes must have the recipients' name and address. We recommend that Congress review statutory obligations that require the printing of SSNs on any documents to determine if the risk of compromise exceeds the value derived, and if so, enact changes to remove these obligations.

My final point is that we should be mindful of the unintended consequences that could result from restricting the use of SSNs among legitimate businesses. Decreasing financial institutions' abilities to use SSNs could potentially lead to increased fraud, increased lending costs, decreased loan approval rates, and a myriad of other unforeseen results. It is important for Congress, the SSA, and other agencies to thoroughly consider the potential consequences and adverse impact such restrictions could have on commerce.

In closing, it is important to note that through BITS, the financial services industry has been aggressive in efforts to mitigate identity theft, reduce fraud, and strengthen cyber security by working together to share information, analyze threats, and implement best practices. We need essential tools such as the CBSV program to continue these efforts.

Thank you for the opportunity to testify before you today. I would be happy to answer any questions.

[The prepared statement of Mr. Stein follows:]

Statement of Erik Stein, Member, BITS Fraud Reduction Steering Committee

Introduction

Good afternoon Chairman McCreery and members of the Subcommittee. My name is Erik Stein. I am Executive Vice President and Director of Fraud Risk Management at Countrywide Financial Corporation, America's largest residential mortgage lender and servicer. I have over 25 years of banking, credit card, mortgage lending and dot com experience and am currently responsible for preventing, detecting, investigating, mitigating and reporting on criminal conduct by, through or within Countrywide and its family of companies.

I am pleased to appear before you today on behalf of BITS and its Fraud Reduction Steering Committee (FRSC) to discuss the role of Social Security Numbers (SSNs) in identity theft and enhancing SSN privacy.

BITS is a nonprofit industry consortium of 100 of the largest financial institutions in the U.S. BITS is the non-lobbying division of The Financial Services Roundtable. BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS' member companies provide fuel for America's economic engine, accounting directly for \$40.7 trillion in managed assets, \$960 billion in revenue, and 2.3 million jobs. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect. BITS focuses on key issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services. BITS' activities are driven by the CEOs and their direct reports—CIOs, CTOs, Vice Chairmen and Executive Vice President-level executives of the businesses.

Especially relevant to today's testimony, the mission of the BITS Fraud Reduction Steering Committee (FRSC) is to identify fraudulent trend activity, reduce fraud losses, and foster new opportunities to reduce the impact of fraud on the financial services industry and our customers. Participants in the BITS Fraud Reduction Steering Committee include representatives from financial institutions, industry associations and the Federal Reserve.

BITS works with government organizations including the U.S. Department of Homeland Security, U.S. Department of the Treasury, federal financial regulators, Federal Reserve, technology associations, and major third-party service providers to achieve its mission.

BITS is also a founding and active member of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). The mission of the FSSCC is to:

- Foster and facilitate the coordination of financial services sector-wide voluntary activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security
- Identify voluntary efforts where improvements in coordination can foster sector preparedness
- Identify barriers and recommend initiatives to improve sector-wide knowledge sharing and timely dissemination of critical information among all sector constituents
- Promote public trust and confidence in the financial services sector's ability to withstand and recover from terrorist attacks, cybercrime, and natural disasters.

The financial services industry has been aggressive in its efforts to strengthen cyber security, reduce fraud, and mitigate identity theft. Members of BITS are sharing information, analyzing threats, creating best practices, urging the software and technology industries to do more to provide more secure products and services, and combating fraud and ID theft. As just one example of these efforts, the Identity Theft Assistance Center (ITAC), which BITS and the Financial Services Roundtable established in 2004, recently announced that it had helped over 5,000 individuals in restoring their financial identity.

SSNs: A Unique Identifier

SSNs have evolved, regardless of original intent, to become the *de facto* unique identifier for consumers. This number is the only unique identifier that today accompanies most consumers from cradle to grave. SSNs remain a constant in an ever-changing world of name change from marriage and divorce, shifting addresses, and driver's license re-issuance as consumers move from one state to another. SSNs are used in efforts to ensure the accurate association of financial accounts, credit reports, public records, medical records and a host of other critical relationships and services to a consumer.

Critical Role of SSNs for Financial Institutions

The use of SSNs by financial institutions is essential to satisfy a variety of statutory obligations such as to report earned interest income and deductible interest payments on mortgages for millions of American consumers. In addition, SSNs facilitate practical realities such as accessing credit reports to determine creditworthiness, performing due diligence on business partners and correspondent banks and, as required by the USA Patriot Act, performing enhanced due diligence on politically-exposed persons (PEP).¹

¹ The Federal Financial Institutions Examination Council's (FFIEC) Bank Secrecy Act Anti-Money Laundering Examination Manual defines a PEP as "a person identified in the course of normal account opening, maintenance or compliance procedures to be a 'senior foreign political

Under the USA Patriot Act, financial institutions are obligated to "know their customer," and to take steps to verify the identity of account holders. In addition, financial institutions perform due diligence on business partners and vendors. One of the integral parts of compliance with these obligations often involves the use of public records which are searched by use of the SSN, or, in the case of business, EIN, to ensure that the results returned are unique to the subject of the due diligence.

After the customer's identity has been verified and the relationship has been established, many financial institutions utilize the SSN internally to track the customer's relationship with the financial institution across multiple accounts and for a variety of legitimate internal business reasons. This legitimate, internal business use should remain exempt from additional limitations.

Criminal investigations initiated by financial institutions are facilitated by the availability of SSNs both in the financial institution's database and in public records. Public records are frequently used by financial institutions' staff during the investigation of potential criminal conduct. During the investigation, the SSN is the single most reliable method of identification, correlation and association of the perpetrators to their public records, which often provide critical details imperative to solving the crime and locating the suspect(s). The loss of this valuable tool would jeopardize the effective investigation of financial crimes.

Financial institutions and other businesses routinely screen prospective employees to verify identity, validate applicant employment and education history, and check for criminal conduct prior to extending job offers. These background checks, particularly in high-risk occupations or vulnerable industries, can reduce the incidence of criminal infiltration, potential workplace violence and security risks, including customer data security and privacy risks. The SSN is critical in verifying a potential employee's background and allows for the ongoing monitoring of employees in high-risk positions. Without the use of a SSN, financial institutions would find it very difficult to adhere to a "know your employee" standard.

SSN Verification: A Key Tool for Successful Identity Determination of Customers

SSNs play a pivotal role in identity determination: the establishment and verification of the identity of unique persons with whom financial institutions, and others, conduct business. With millions of John Smiths in America, the identity determinate of which John Smith with whom a financial institution is dealing is made by the single unique identifier common to all Americans, his SSN.

Importantly, financial institutions realize that the ability to successfully verify John's SSN is not the same as successfully determining his identity. A financial institution must do this through the use of identification documents such as driver's license, passport and other, typically government-issued, identity documents containing a picture, signature, expiration date, security features, a physical description, etc. It should be noted that SSNs have not been used for identity verification due to the lack of a highly secure SSN card, tamper-proof signature, picture and expiration. The SSN card contains few security features making it easy to counterfeit and reducing or eliminating any value in its use for identity verification. The SSN is thus only a tool, albeit an invaluable one, in the process of determining the identity of an individual. It is clear, however, that verification is a key tool for achieving positive identity determination.

Value of the SSN to Criminals

The critical role of SSNs is the fundamental reason for their intrinsic value to criminals' intent on committing crimes. Criminals utilize SSNs in the commission of identity theft. Identity Theft may be divided into "true name" fraud where the perpetrator uses the "true" identity of a consumer, or identity fraud where combinations of consumer's identities are pieced together or even fabricated to create a synthetic identity, a new person.

It is important to recognize that criminals committing identity fraud don't need to steal or purchase SSNs to commit their crime. The structure of the SSN is common knowledge to anyone who has ever had, or seen, one or checked the Social Security Administration's (SSA) website (i.e. <http://policy.ssa.gov/poms.nsf/lnx/0100201030?opendocument>.) Valid SSNs can be determined by checking the SSA's website for the highest group issuance <http://www.socialsecurity.gov/employer/highgroup.txt>. By selecting a recently issued SSN, and applying for credit, a criminal creates an identity with the Credit Reporting Bureaus (for which there will be no conflicting SSN information since the valid SSN holder is an infant).

figure,' any member of a senior foreign political figure's 'immediate family,' and any 'close associate' of a senior foreign political figure."

Since financial institutions and lenders don't have the ability to verify the SSN, name and date of birth combinations (other than the current Enumeration Verification System pilot in the mortgage industry which is not a robust, enterprise-strength, low cost, timely verification process and therefore narrowly used), the identity thief is unlikely to be caught. Restrictions on the sale and purchase of SSNs would do little to prevent this type of fraud. The fraud also doesn't rely on the theft of SSNs from their legitimate owner.

BITS members would encourage the Subcommittee to remove the highest group issuance list from the public domain and make it available to financial institutions and others with a legitimate business need on a subscription basis as is currently done with SSA's Death Master File. While this list is an essential tool today to validate SSNs provided to financial institutions, its potential use by criminals is inconsistent with its availability to the general public.

Another area of risk is that criminals in search of identities for committing true name fraud can readily obtain name, address, SSN and account number combinations by mail theft during January each year when millions of account holders and borrowers receive their 1099's or 1098. By statute, these tax forms are required to display the account holder's SSN, and, for mailing purposes, must have the recipient's name and address along with the account number to identify the account for which the form has been filed. These forms are mailed *en masse* by financial institutions at the beginning of the year for use in requisite income tax filing by the consumer thereby making for a target-rich environment for obtaining identities through mail theft.

Combating Identity Theft through SSN Verification

For decades, financial institutions have required SSNs and identity documents to open accounts, make loans and accept transactions by their customers. However, the industry has been relegated to validation methods that do not, and cannot, validate the existence of, and their association with, a consumer's personal identifiers (such as name, date of birth and gender). For SSNs, financial institutions have relied on rules that determine if the SSN had been issued (the highest group issuance list referenced above available from SSA), that the SSN holder had not been reported deceased (SSA's Death Master File), and that the holder was not born after the issuance of the SSN by SSA (from historical highest group issuance lists). The single most important validation has been unavailable, that the consumer presenting the number is the holder of record in SSA's database.

The proposed Consent-Based SSN Verification (CBSV) program recently published for public comment by the SSA is an extension of the Enumeration Verification System pilot and is a critical effort to allow financial institutions to verify SSNs. It will allow financial institutions to verify the SSN holder's name and date of birth against SSA's database. Establishing a system capable of high volume, low cost, real time verification direct to financial institutions and lenders would significantly reduce the incidence of synthetic identities. "True name" identity theft would become more difficult with the validation of date of birth and the optional gender code by financial institutions utilizing a CBSV program.

BITS' members strongly encourage the Subcommittee to support the CBSV program.² We also request that the SSA evaluate the removal of restrictions on the daily volume of submissions by participants, work towards improving the proposed response times, eliminate requirements for a standalone consumer authorization allowing incorporation of the authorization into loan or account documents, and review the cost structure.

Consumers would benefit from industry's ability to verify SSN information by reducing the incidence of fraud and errors. Erroneous data entry of consumer's SSNs would also be easily determined, reducing the incidence of erroneous tax reporting on interest earned and deductible interest expense and reducing the quantity of consumers required to be subjected to annual solicitation for a corrected SSN due to mismatches submitted to the IRS and misrepresentation.

Further, the BITS members, due to the high perceived value of CBSV, would also encourage the consideration of federal legislation to mandate similar programs related to other governmental identity documents used in the financial industry to verify consumers including U.S. passports, alien registration documents (e.g. Non-Resident Alien card) and state driver's licenses. Financial institutions, while under obligations to know their customer under the USA Patriot Act, have not been afforded the tools to ensure the validity of the documents presented for identity verification. We have had to rely exclusively on the appearance of legitimacy (e.g.

² Attached is the BITS/Financial Services Roundtable Comment Letter on the Social Security Administration's Consent-Based Social Security Verification Process (February 2006)

verification of security features, visual inspections or tests that validate the structure of a driver's license number but, again, not the name of the true license holder).

Unintended Consequences for Limiting Use of SSNs

The critical roles of SSNs for use in financial institutions, investigations, public records, lending, account servicing, tax reporting and much more makes the availability and use of the SSN for legitimate business uses an imperative. It is important that additional proposed restrictions on the use, sale and purchase of SSNs be thoroughly evaluated to ensure that unintended consequences do not occur. This could include potential increases in fraud; economic impacts from increased lending costs; and decreased loan approval rates and other adverse implications to commerce.

Conclusion and Recommendations

In summary, the use of SSNs is critically important to the financial services industry. They allow financial institutions to meet various statutory obligations such as knowing who their customers, employees, and business associates are; reporting earned interest income and deductible interest payments on mortgages; and satisfying due diligence expectations as set forth by statutory obligations. All of these functions are performed to keep our customers and their financial assets safe, and to ensure the security and reliability of the economy.

On behalf of BITS and our member financial institutions, we encourage Congress to:

- Continue to allow financial institutions to use SSNs without additional restrictions and limitations;
- Exercise caution if changes are considered, to be especially alert to unintended consequences such as increased fraud;
- Support a verification program capable of high volume, low cost, real time verification in a manner consistent with customers' demands; and
- Review statutory obligations that require the printing of SSN's (e.g. 1098, 1099) to determine if the risk of compromise exceeds the value derived and, if so, enact changes to remove these obligations.

Thank you for the opportunity to testify before you today. I would be happy to answer any questions.

February 26, 2006

Office of Management and Budget (OMB)

Attn: Desk Officer for SSA

Fax: 202-395-6974

Social Security Administration, DCFAM,

Attn: Reports Clearance Officer

Fax: 410-965-6400

E-mail: OPLM.RCO@ssa.gov

Re: Comment to Consent Based Social Security Number Verification (CBSV) Process

Dear Sirs and Madams:

BITS and The Financial Services Roundtable appreciate the opportunity to participate in the Social Security Administration's (SSA) request for comment regarding the Consent Based Social Security Number Verification (CBSV) Process.

BITS and The Financial Services Roundtable share membership and represent 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. BITS works to leverage the intellectual capital of its members, fostering collaboration to address emerging issues where financial services, technology, and commerce intersect. The Roundtable promotes the interests of member companies in legislative, regulatory and judicial forums. Roundtable member companies provide fuel for America's economic engine, accounting directly for \$40.7 trillion in managed assets, \$960 billion in revenue, and 2.3 million jobs.

Our members have always been a favorite target for perpetrators of fraud. Institutions have long answered this challenge with reliable business controls, advanced technology, information sharing, and cooperative efforts with government and law enforcement agencies. While our members' foremost concern is to protect their customers and maintain their trust, they are also mindful of the need to comply with the regulations set forth by Section 326 of the Patriot Act. This section requires in-

stitutions to verify not only the identity of a customer, but also the accuracy of the information provided.

In the interest of reducing fraud and complying with Section 326 of the Patriot Act, BITS members supported the initial pilot, the Enumeration Verification System (EVS), to allow institutions to affirmatively verify consumer's name, social security number and date of birth (DOB). This pilot provided a means to ensure accounts were opened for the legitimate consumer and not a "fraudster" and we applaud the SSA's efforts to provide enhancements in the form of the CBSV that would benefit our customers and our industry.

After careful review of the information collection process outlined in the December 30, 2005 Federal Register, we respectfully offer the following comments:

"Valid Consent from Number Holders"

There is concern that, since the CBSV is designed to verify a person's Social Security Number (SSN) to their name (and potentially DOB), there may be instances where financial institutions are misled and the consent is not from the true applicant as may be the case in identity theft or identity manipulation. There should be acknowledgement that while financial institutions have established a process for verification, there is still an opportunity for applicants to provide false information. This verification process is fundamental to ensuring the name, SSN, and DOB (optionally) match the authorizing consumer. While we understand the use of "valid consent from number holders," we want to ensure that there are no consequential impacts to financial institutions from the fraudulent completion of consent authorizations.

Inclusion of Gender Code

The public comment details the submission as consisting of a name, SSN and DOB (if available) and the results provide a match to name, SSN, date of birth and gender code (which is not part of the submission). Clarity needs to be provided on whether gender code is intended to be a submitted/verified field.

Full Name Matching

While SSN, DOB (and possibly gender assuming it is used) are unique variables, one's name is subject to wide variation. It is suggested that the full first and full last be used for matching and that a secondary field be available for each that could include a nickname, shortened name (Jim vs. James) and last name. The use of a secondary field for name matching would reduce the incidence of re-running queries; improve match rates including where Soundex matching is utilized and the name variation is not conducive to such matching logic; and would accommodate name changes due to marriage, divorce, etc. which may not yet have been reported to SSA.

Real-time vs. Batch Submissions

SSA had indicated its intention to continue the practice of EVS in providing the results of inquiries by Requesting Parties within 48 hours while not guaranteeing such response time. Institutions believe there is strong value in having real-time capabilities and encourage the SSA to evaluate methods to provide this verification service in real-time as soon as feasible. If batch submissions remain exclusively available, members strongly encourage SSA to provide a response, to inquiries submitted before midnight, by no later than 5am the following business morning consistent with other batch jobs run by financial institutions for fraud detection, verification and posting.

Daily Limitation of Records and Expectation of Volume

While strongly supportive of CBSV, we urge the SSA to reconsider the daily limitation of 5,000 records. One of the inherent values of an automated system of SSN verification is its scalability. With scalability in mind, we recommend the SSA remove the daily limitation.

Should hardware limitations be reached by the overwhelming success and adoption of CBSV, the SSA should charge registered user businesses sufficient additional fees to allow the SSA to meet this demand. This linear scalability should also keep the cost per inquiry low. We believe that SSA's expectations of demand for CBSV are substantially below the industry's need for this verification solution. We encourage the SSA to revise its expectations and lower the cost of entry for business by reducing the initial fee of \$40,288.10. While the basis for SSA's expectation of only 150 business users for CBSV is not explained in the publicly available documents, we believe that, with nearly 9,000 FDIC-insured financial institutions alone in the U.S., 5,000 business users is both reasonable and sustainable. This would lower the initial cost of entry to \$1,208.64. However, to both encourage maximum participa-

tion and guarantee SSA's financial support of the program, we recommend the initial fee be set at \$10,000.

Document Requirements

SSA-89—Authorization for the Social Security Administration (SSA) To Release Social Security Number (SSN) Verification

Evidence of consumer authorization to verify their SSN is clearly both an obligation of the Requesting Party and a necessary privacy safeguard. However, the requirement for a standalone SSA-89 evidencing said authorization provides no additional safeguard over an obligation for equivalent language, approved by the SSA prior to usage, incorporated into account or loan documents. In addition, this document (SSA-89) cannot be incorporated into loan documents, account signature cards or any other documents. For efficiency and enhancement purposes, institutions must be able to incorporate the authorization language into existing documents that allows them to run the SSN which can then be retained for six years from the authorization date.

The existing retention of these underlying documents already, in most cases, meets or exceeds the SSA minimum retention requirement. Where the existing document retention is shorter than SSA-89's retention requirement, Requesting Parties will voluntarily comply with modification of their retention schedules to achieve the efficiencies afforded by merging these documents with the CBSV authorization. The SSA should consider inclusion of specific authorization of the SSN owner for electronic signature in accordance with the Electronic Signatures in Global and National Commerce Act (ESIGN). SSA's existing allowance of storage of the SSA-89 electronically would be consistent with the use of ESIGN for electronification of the authorization process with inherent increased efficiency.

SSA-89 cannot be modified by the Requesting Party. The defined term can be modified by agreement as specified in the User Agreement, by agreement of the parties executing the Authorization and documented therein. These two statements are mutually exclusive. We recommend SSA clearly delineate the method by which Authorization term extension is to be documented so the Requesting Party can ensure compliance with SSA's requirements.

SSA-88—Pre-Approval Form for CBSV

The Requesting Party has a contractual obligation to protect the integrity of SSA's systems, utilize information requested only for authorized purposes, and to be authorized by the Requesting Party in accordance with their internal approval policies. The need for completion of form SSA-88 for each employee in a large company that has access to the results of the inquiry is overly burdensome and inefficient. We strongly encourage the SSA to make user administration for Requesting Parties an obligation of authorized employees of the Requesting Party and managed through a user interface in Business Services Online (BSO). All service providers to the financial services industry allow the participant to manage their employees' access. The BSO administrative user interface can be designed so as to require the data elements mandated by SSA (e.g. name, SSN, phone number, and email address of each employee) with appropriate electronic attestation by the authorized admin user during new user setup. Maintenance (e.g. changes to the existing information as a result of job status changes, phone or email changes) and deletion (e.g. termination of the employee or job status changes no longer requiring access) can likewise be accomplished through the BSO administrative user interface by the authorized employee of the Requesting Party. This process is much more conducive to large scale employers who may have thousands of employees authorized to access the information from SSA during the processing of accounts or loans.

SSA-1235—Agreement Covering Reimbursable Services

SSA-1235 is "effective upon signature of both parties and shall remain in effect until one or more of the following events occur. . . ." While the Agreement is continuously in effect (barring one of the events listed), SSA requires an annual resubmission of the Agreement. The resubmission appears inconsistent with an Agreement with no defined term. We recommend the SSA eliminate the annual submission requirement for form SSA-1235. The provision of the annual fee as defined by SSA each year should be sufficient evidence of the Requesting Party's intent to continue the Agreement. The Conditions of Agreement, paragraph 6, stipulates that the Authorization "must be presented within 60 days after its execution," however the Authorization itself indicates it "is valid only for 90 days from the date signed. . . ." These statements are incongruous and we recommend the SSA reconcile these documents to a consistent period of 90 days. The Conditions of Agreement, paragraph 8, stipulates the Agreement may be terminated "by giving a 60 day advance written

notice." However, Section XI. *Duration of Agreement, Suspension of Services, Annual SSA-1235* of the User Agreement specifies "the Agreement shall terminate 30 days after the date of the notice or at a later date specified in the notice." We recommend the SSA reconcile this discrepancy by establishing a consistent 30 day written notice requirement for termination.

Submission of Requests

The CBSV User Guide establishes the file format for submission of requests by the Requesting Party to SSA. The file format contains a field for a "Multiple Request Sequence Number"; however, the SSA limits the number of file submissions by a Requesting Party to one. Since only one file can be submitted daily, there would never be a need for this field. If the field is anticipated for future use when Requesting Parties may be allowed multiple daily file submissions, we suggest "Future Use" indicated in the description for this field to remove ambiguity.

If you have any further questions or comments on this matter, please do not hesitate to contact us or Heather Wyson at (202) 289-4322.

Sincerely,

Catherine A. Allen
CEO, BITS

Richard M. Whiting
Executive Director and General Counsel

Chairman MCCRERY. Thank you, Mr. Stein. Mr. Pratt?

STATEMENT OF STUART K. PRATT, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CONSUMER DATA INDUSTRY ASSOCIATION

Mr. PRATT. Mr. Chairman and Members of the Committee, thank you for this opportunity to appear before you today to discuss the importance of SSNs. For the record, my name is Stuart Pratt and I am President and CEO of the Consumer Data Industry Association.

We applaud this Committee for the thoughtful and open dialog regarding how SSNs are used and to identify risks associated with such use. Before I discuss how our members' systems make use of the SSN, let us just consider how demographics in our society really explain why the SSN is so important.

First, identifiers in everyday life do change and do so more often than we might think. Over 40 million addresses change every year in this country. More than three million last names change due to marriage and divorce. We use our identifiers inconsistently. We don't do so purposefully, but a simple example is our choice to use a nickname in some transactions but to use our full name in others. Our name is not as unique as we might think. There are millions and millions of Smiths and Joneses in this country, and, in fact, more than 13 million consumers have only one of ten very common last names. Another 57 million males have only one of ten common first names.

We provide other examples of how personal information changes in our written testimony, and by taking into account all of these facts, it really does become very apparent why the SSN is the key to stabilizing consumers' identifying information in the context of databases. The SSN is truly a unique identifier.

Let us discuss how the use of the SSN works within our members' systems. Our members design products for determinations of a consumer's eligibility for a product or service, to prevent fraud,

and to aid in the location of consumers for a variety of reasons. These products bring great value to us as consumers every day. Eligibility products, such as a credit or employment report, for example, lead to definitive decisions.

These reports are regulated under the Fair Credit Reporting Act (P.L. 91-508). The FCRA imposes a duty that consumer reporting agencies employ reasonable procedures to ensure the maximum possible accuracy of the information in the report, and the SSN plays a vital role in helping our members to achieve this maximum possible accuracy standard. Absent the use of the SSN as a key identifier, consumers would be harmed in many ways through the exclusion or inclusion of information.

Our members also produce products regulated under other laws, such as the Gramm-Leach-Bliley Act. Fraud prevention systems, for example, employ a diversity of strategies. The SSN plays an important role. In 2004 alone, businesses conducted more than 2.6 billion searches to check for fraud. The largest users of fraud detection systems are, in fact, financial services companies, accounting for about 78 percent of the transactions, but there were others users. 5.5 million location searches were conducted by child support enforcement agencies, 378 million searches to enforce contracts to pay, tens of millions of searches were used by pension funds, blood donor organizations, and by organizations focused on missing and exploited children. The availability and permitted use of the SSN remains vital across this entire spectrum of consumer data products.

Consumers and media often assume that the SSN is fully unregulated and, of course, this is not the case. As we have discussed, laws such as the FCRA and the Gramm-Leach-Bliley Act do regulate our members' products. However, we recognize that similar protections don't exist for all, and the SSN is sensitive personal information that must be protected. We believe that a national uniform system to establish information safeguards should be enacted so that anyone possessing sensitive personal information, such as an SSN in combination with my name and address, that they would be obligated to protect that information. There are a number of House and Senate committees that are looking at proposals.

I think standards like this would cause more American businesses to move to encrypt such information, which we think is the right direction. I think other businesses would decide whether or not they really should be gathering it in the first place. We think that is another good result, as well. Our members want to protect that information. We think every company and every business in this country that is going to gather that information should do the same.

Public records also contain SSNs, and it is encouraging to hear the State court organizations discussing strategies to protect them. We support this effort unequivocally. However, CDIA does believe that the disclosure of the SSN to the general public, while it must be addressed, we also believe that public records must be made available, including SSNs, to those with appropriate needs. Public records play a vital role in our society and they bring value to consumer data industry products and services. Bankruptcy records, for example, and tax liens as well as judgments are used by lenders.

Records of eviction are critical to a landlord, and these are just a few examples.

The public sector agencies are taking actions and we are encouraged by SSA's efforts to explore the viability of a system by which a party may verify a particular SSN is associated with another. However, the system is cumbersome. It does not allow for real-time automated processing of SSN verification and it will render it very ineffective, in fact, in assisting victims of identity theft. We hope the SSA will move toward a more effective system in the future.

In conclusion, we believe that enacting law that imposes national uniform information security regulations on all who possess the SSN is the right step to take and this is the right year in which to do it. In contrast, laws that overreach and attempt to limit the SSN's use are likely to merely take fraud prevention tools off the table and out of the hands of legitimate businesses and expose—and ultimately at the expense of consumers. We believe consumers expect us to protect the SSN. We also know consumers expect us to maintain accurate databases. Thank you, Mr. Chairman.

[The prepared statement of Mr. Pratt follows:]

**Statement of Stuart K. Pratt, President and Chief Executive Officer,
Consumer Data Industry Association**

Chairmen McCrery, Ranking Member Levin and members of the committee, thank you for this opportunity to appear before you today to discuss the importance of Social Security Numbers to our members' consumer data systems. For the record, my name is Stuart Pratt and I am president and CEO of the Consumer Data Industry Association.¹ Our members applaud this committee for the thoughtful and open dialogue it has sought regarding how Social Security Numbers are used and to identify risks associated with such use.

OVERVIEW

Before I discuss how our members' systems make use of the social security number, it is important to take into account key demographics about our society that help explain why the SSN so important.

Personal identifiers change:

While it probably doesn't occur to most of us, the identifiers we use in everyday life do change and more often than most might think. For example, data from the U.S. Postal Service and the U.S. Census confirm that over 40 million addresses change every year. More than three million last names change due to marriage and divorce. While trends in naming conventions are changing, this fact is still far more often true for women than men.

We use our identifiers inconsistently:

It is a fact that we use our identifiers inconsistently for a wide variety of reasons. First, many citizens choose to use nicknames rather than a given name. However, there are times where, in some official transactions, a full name is required. Some consumers, when hurried, use an initial coupled with a last name, rather than their full name or nickname. Consumers are also inconsistent in the use of generational designations (e.g., III, or Sr.). Finally, there are times where consumers themselves do make mistakes when completing applications. Thus, a consumer's identifiers may be presented in different ways in different databases and, in some cases, the data may be partially incorrect.

Personal identifiers are not always unique:

We think of our names as a very personal part of who we are. However, our names are less common and unique than we might think. For example, families

¹ CDIA, as we are commonly known, is the international trade association representing over 300 consumer data companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services, systems for insurance underwriting and also collection services. As we will discuss below, the secure and protected use of the social security number (SSN) is an important key to the effectiveness of these systems and services.

carry forward family naming conventions leading to some consumers sharing entirely the same name. Further, U.S. Census data shows that both first and last names are, in some cases amazingly common. Fully 2.5 million consumers share the last name Smith. Another 3 million share the name Jones and more than thirteen million consumers have one of ten common last names. First names are also used very commonly leading to common naming combinations. Eight million males have either the name James or John and a total of 57 million males have one of ten common first names. An additional 26 million females have one of ten common first names. Common naming conventions make it more difficult and in some cases impossible to depend on name alone to properly match consumer data.

Identifiers are shared:

Our birthday is a unique day in our lives, but it is, nonetheless, a date shared with hundreds of thousands of others. Date of birth alone is not an effective identifier. Family members who live together end up sharing addresses and per our discussion above, where consumers share the same name due to family traditions and the address at which they live, distinguishing one consumer from another is complex.

Data entry errors do happen:

Hundreds of millions of applications for credit, insurance, cellular phone services, and more are processed every year. There is no doubt that in the process of entering a consumer's identifying information errors can be made which carry forward into databases and into the reporting of data to consumer reporting agencies.

By taking into account all of these facts about our identifying information, it becomes far more apparent why the SSN is key in stabilizing a consumer's identifying information in the context of databases. The SSN is a truly unique identifier.

USE OF THE SSN BY CDIA MEMBERS

CDIA's members produce a range of critical consumer data products which bring great value to individual consumers, to society and the nation's economy. Our members design products used for determinations of a consumer's eligibility for a product or service, to prevent fraud and to aid in the location of consumers for a variety of reasons.

Consumer Data Products Used for Eligibility Decisions

Many CDIA-member products are focused on helping consumers to gain access to the goods and services for which they apply. These transactions focus on a consumer's eligibility and, as such, the consumer data products used are regulated under the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*) as "consumer reports." Eligibility determinations include applications for any type of credit including unsecured credit, home purchases, auto financing, home equity loans, as well as for insurance of all types, employment, government benefits, apartment rentals, and for other business transactions initiated by the consumer.

The FCRA, enacted in 1970, has been the focus of careful oversight by the Congress resulting in significant changes in both 1996 and again in 2003. There is no other law that is so current in ensuring consumer rights and protections are adequate.

Of particular importance to our discussion here today, is the FCRA-imposed duty on consumer reporting agencies by the FCRA (and similar state laws) that reasonable procedures be used to ensure the maximum possible accuracy of the information contained in all types of consumer reports. This duty is established for the protection of consumers. The SSN plays a vital role in helping our members to achieve the "maximum possible accuracy" standard.

Absent use of the SSN as a key identifier, consumers would be harmed in many ways. Consider the following illustrative examples:

- **Incomplete data harms consumers:** There would be a likely increase in the inability of consumer reporting agencies to properly match incoming information to the correct consumer about whom the information relates. Think about the consequence to consumers of having a consumer "credit" report that does not contain all of the accounts that they pay on time and which makes them eligible for the lowest cost loans.
- **Incomplete data harms our banking system:** The absence of the SSN would also put at risk the safety and soundness of lending decisions due to less information being included in consumer "credit" reports due to data matching problems.
- **Incomplete data prevents consumer access to goods and services:** Think about the consequence for consumers when a consumer reporting agency cannot

locate the proper file on a consumer and thus a lender, insurer or other service provider wanting to do business with the consumer has to deny the application.

There is no doubt that consumer reporting agencies of all types provide tremendous benefits to consumers directly and to the nation's economy and the use of the SSN in the context of our members' systems helps bring forward these benefits. Consider the following:

- **Access to home ownership:** Every homeowner benefits from a credit reporting system that reduces the costs of all mortgage loans by a full two percentage points, thus putting literally thousands of dollars in disposable income into their pockets.² Homeownership is no longer a luxury of the well-to-do, but is a truly democratized American dream enjoyed by nearly seventy percent of the population.³
- **Check fraud prevention:** Check fraud is reduced thanks to CDIA members' systems. It is estimated that more than 1.2 million worthless checks enter the payment system every day in the United States. This number speaks to the risks, but also the success of our members' systems which service as many as 40 billion check transactions a year.
- **Tenant screening services:** Tenant screening services help all landlords to make informed decisions, as well. Consider the circumstances of a retiree who owns a rental property on which he or she depends for income. A tenant screening service mitigates risks for literally millions of such individuals in a country where the majority of units for lease are owned by individuals and not by corporations.
- **Employment/security screening:** SSNs serve as vital links among disparate records that help businesses verify prospective employees' identities and conduct thorough, accurate background checks to ensure workplace safety and business security. Our members' systems and services help to ensure that hardened criminals and sex offenders do not end up working at daycare centers, schools, nuclear power plants, or secure-ID areas of airports.
- **Small business B-to-B transactions:** An SSN is the key business entity identifier to virtually all sole proprietorships or partnerships. As a result, SSNs are required to facilitate business-to-business transactions between small businesses.
- **Securitized credit markets:** Confidence in the U.S. securities market is made possible by accurate financial histories compiled using the SSN as a key identifier. Restricting use of the SSN could undermine confidence in these securities, resulting in substantially higher consumer costs for credit, including mortgages and auto loans.
- **Investigative services and insurance fraud:** SSN access is an important tool for investigative services and insurance fraud investigation. Insurance fraud losses are estimated to exceed \$79 billion a year—\$900 per family—in the U.S. Prohibiting use of SSNs for investigative purposes could drive those costs even higher.

Consumer data products used for fraud prevention and location

Not all CDIA member products are used for an eligibility determination, but products regulated under other laws such as the Gramm-Leach-Bliley Act (Pub. L. 106-102, title V) are used in critical ways for the benefit of all consumers. CDIA's members represent the leading companies in the field of consumer identity verification, fraud prevention and location services.

Fraud prevention systems:

Fraud prevention systems deploy a diversity of strategies, but clearly the SSN plays an important role. In fact, in 2004 alone, businesses conducted more than 2.6 billion searches to check for fraudulent transactions. As the fraud problem has grown, industry has been forced to increase the complexity and sophistication of the fraud detection tools they use. As the importance of fraud detection tools increases, the potentially negative consequences of allowing "access and correction" to these databases must be considered in order to protect the accuracy of the included data, and thus the overall integrity of these tools.

²Kitchenman, Walter., *U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns*, Pp. 5 (1998).

³Turner, Michael., *The Fair Credit Reporting Act: Access, Efficiency & Opportunity*. Pp. 8 (2003).

How do Fraud Detection Tools Work?

Fraud detection tools are also known as Reference, Verification and Information services or RVI services. RVI services are used not only to identify fraud, but also to locate and verify information for public and private sector uses. While fraud detection tools may differ, there are four key models used.

- **Fraud databases**—check for possible suspicious elements of customer information. These databases include past identities and records that have been used in known frauds or are on terrorist watch lists, suspect phone numbers or addresses, and records of inconsistent issue dates of SSNs and the given birth years.
- **Identity verification products**—crosscheck for consistency in identifying information supplied by the consumer by utilizing other sources of known data about the consumer. Identity thieves must change pieces of information in their victim's files to avoid alerting others of their presence. Inconsistencies in name, address, or SSN associated with a name raise suspicions of possible fraud.
- **Quantitative fraud prediction models**—calculate fraud scores that predict the likelihood an application or proposed transaction is fraudulent. The power of these models is their ability to assess the cumulative significance of small inconsistencies or problems that may appear insignificant in isolation.
- **Identity element approaches**—use the analysis of pooled applications and other data to detect anomalies in typical business activity to identify potential fraudulent activity. These tools generally use anonymous consumer information to create macro-models of applications or credit card usage that deviates from normal information or spending patterns, as well as a series of applications with a common work number or address but under different names, or even the identification and further attention to geographical areas where there are spikes in what may be fraudulent activity.

Who uses Fraud Detection Tools?

The largest users of fraud detection tools are financial businesses, accounting for approximately 78 percent of all users. However, there are many non-financial business uses for fraud detection tools. Users include:

- **Governmental agencies**—Fraud detection tools are used by the IRS to locate assets of tax evaders, state agencies to find individuals who owe child support, law enforcement to assist in investigations, and by various federal and state agencies for employment background checks.
- **Private use**—Journalists use fraud detection services to locate sources, attorneys to find witnesses, and individuals use them to do background checks on childcare providers.

Location services and products

CDIA's members are also the leading location services providers in the United States. These services, which help locate individuals, are a key business-to-business tool that creates great value for consumers and business alike. Locator services depend on a variety of matching elements, but again, a key is the SSN. Consider the following examples of location service uses:

- There were 5.5 million location searches conducted by child support enforcement agencies to enforce court orders. Access to SSNs dramatically increases the ability of child support enforcement agencies to locate non-custodial, delinquent parents (often reported in the news with the moniker "deadbeat dads"). For example, the Financial Institution Data Match program required by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PL 104-193) led to the location of 700,000 delinquent individuals being linked to accounts worth nearly \$2.5 billion.
- There were 378 million location searches used to enforce contractual obligations to pay debts.
- Tens of millions of searches were conducted by pension funds (location of beneficiaries), lawyers (witness location), blood donors organizations, as well as by organizations focused on missing and exploited children.

Clearly location services bring great benefit to consumers and to businesses of all sizes. Availability and permitted use of the SSN remains vital to the effective operation of these services for both private and public sector purposes.

INFORMATION SECURITY AND THE SSN

Because of recent media coverage regarding security breaches of sensitive personal information and also general concerns about identity theft, some consumers

may well feel that data about them presents risks that outweigh benefits. But in reality as we have discussed above, there is clear and convincing value in the uses of such data, including the SSN, that bring direct value to consumers and our nation's economy, which must be preserved.

Consumers and media often assume that use of the SSN is wholly unregulated and this is not the case. As we've discussed, the FCRA regulates SSNs in the context of consumer reports and our members' use of the SSN is also regulated under the restrictions of the GLB. Other laws such as the Fair Debt Collection Practices Act (15 U.S.C. 1601 *et seq.*), the Health Insurance Portability and Accountability Act (Pub. L. 104-191), and the Drivers Privacy Protection Act (18 U.S.C. 2721 *et seq.*), also impose protections on sensitive information about consumers which in turn protects the SSN.

However, CDIA's members recognize that the laws which cover them may not extend to all and clearly the SSN is sensitive personal information which must be protected. The following statement delivered during our testimony before the Senate Banking Committee on September 22, 2005 continues to reflect our position on protecting sensitive data about consumers, including the SSN:

"The discussion of safeguarding sensitive personal information and notifying consumers when there is a substantial risk of identity theft has expanded beyond the boundaries of financial institutions. It is our view that rational and effective national standards should be enacted both for information security and consumer notification as it applies to sensitive personal information, regardless of whether the person is a 'financial institution.'"

As this committee knows, there are a number of House and Senate committees that are focused on developing uniform national standards for ensuring the protection of sensitive personal information. We believe that enactment of national standards will ensure that the SSN is protected by all who possess it. New nationwide safeguards regulations authored by the Federal Trade Commission will compel all to deploy physical and technical strategies for the protection of sensitive information about consumers. Further they will likely cause American businesses to move to encrypt such information and finally some will question why they gather the SSN in the first place. Further, information safeguards rules would effectively bring into question the business model of operating publicly available websites that sell a consumer's SSN to virtually anyone who is willing to pay the price.

Ultimately national standards for the safeguarding of the SSN and other sensitive personal information will address consumer concerns and perceptions. These are all good public policy results and CDIA remains committed to a constructive dialogue as various bills move through the House and Senate.

PUBLIC RECORDS AND THE SSN

The historical debate about the presence of the SSN in public records has suggested a binary proposition of either providing everyone with access to all of a record, including the SSN, or to deny all access to the record with an SSN. We think that this paradigm is dated and today encouraging trends in the technologies used to make public records available to all citizens, particularly via the internet, are allowing state and federal agencies to employ far more sophistication in how and when an SSN will be disclosed.

It is also encouraging to hear state court organizations discussing strategies for protecting SSNs and CDIA will continue to engage in these dialogues. However, while CDIA believes that disclosure of the SSN to the general public must be addressed, we also believe that public records must be made available, including SSNs, to those with an appropriate need. States are seeking out dialogue with the private sector about future access to public records which shows promise. Consider the following excerpt from CDIA's April 18, 2002 letter to the National Center for State Courts:

"... consider the example of the Maryland court access project that tried to create a limitation on bulk access to court records. The concerns raised at a public hearing in December 2000 'prompted [Chief] Judge Bell to appoint an expanded, more representative task force.'⁴ The expanded task force recently issued a final report and noted that requestors of bulk data sell that information 'with value added' to their customers. The report also noted that registration agreements between the court and the bulk data requestors 'can provide a vehicle for reasonable safeguards concerning released data.'⁵

⁴ Maryland Judiciary Website (visited March 20, 2002).

⁵ Report of the Maryland Court of Appeals Committee on Access to Court Records 10 (Feb. 2002).

Public records play a vital in our society and bring value to the consumer data industry's members. Bankruptcy records, tax liens and judgments are part of consumer "credit" reports used by lenders to make decisions that implicate safety and soundness. Records of eviction are critical to landlords who must themselves pay the bills and attempt to lease properties to consumers who will do the same. Validating professional licenses for employment screening agencies is yet another use of public records, as is accessing criminal histories.

Through the development of nationwide databases of public record information, our members have solved the problems inherent in having to search through tens of thousands of federal and state court houses and agency databases. In this way, the SSN is as important an identifier in a public document as it is in a private-sector database. It is a critical identifier for all of the data management reasons we discuss above. Without an SSN, a consumer can simply alter a few items of information, such as moving to a new address, or even changing a name and thus separate himself/herself from a bankruptcy record, a tax lien, a record of eviction and even a criminal history, in some cases. Clearly this is not a positive outcome for consumers or for American businesses which are on the front lines of making, for example, fair and accurate risk-based lending and employment decisions, while at the same time fighting identity theft and fraud.

Some federal proposals have suggested that state agencies must limit access to the SSN. The concern of the CDIA's members is that this apparent unfunded mandate will drive under-funded state agencies to either stop requesting the SSN when processing vital records, or to simply deny all access to the SSN for a variety of reasons including the fact that they cannot fund a bifurcated system of access to the SSN for some but not for others. Additionally, because some state public access laws appear to prohibit a bifurcated approach.

Ultimately, dialogue with state and federal agencies coupled with the advancement of technologies will address concerns about public records which contain SSNs. An unfunded mandate will destabilize the system of public records which is so important to our democracy.

In the context of discussing governmental agencies and the SSN, we do want to acknowledge and are encouraged by the Social Security Administration's efforts to explore the viability of a system by which a party may verify that a particular SSN is associated with a particular name. A discussion of this system can be found in the December 30, 2005 edition of the *Federal Register*, Vol. 70, No. 250. Entitled "Consent Based Social Security Number Verification Process," the service will be available starting June 2006 and only a limited number of parties are allowed to enroll. As it currently stands, this system is very cumbersome and does not allow for a real-time automated process of SSN verification which will render it very ineffective for assisting victims of identity theft and also preventing the crime. We hope that the SSA will move towards a truly automated, system that meets the broader needs of the data industry.

CONCLUSION

In conclusion, you can see that the underlying theme in the discussion of SSN uses is that of balance and ultimately ensuring the security of the number. Law that imposes national uniform information security regulations on all who possesses the SSN in combination with a person's name and address, is the most responsible and constructive focus for Congress. In contrast, law that overreaches in attempting to limit use of the SSN is likely to merely take fraud prevention tools out of the hands of legitimate businesses at the expense of consumers. Ironically, to prevent fraud you must be able to crosscheck information. To maintain accurate databases, you must be able to maintain a range of identifying elements. Absent the availability of the SSN, we will be less able to build accurate data bases, to accurately identify records and to help prevent identity theft through the development of fraud prevention and authentication tools. Ultimately consumers expect us all to accomplish the goals of protecting and securing the SSN, and also ensuring the accuracy and effectiveness of databases which contain information about them.

Thank you for this opportunity to testify.

Chairman MCCRERY. Thank you, Mr. Pratt. Mr. Hulme?

STATEMENT OF BRUCE H. HULME, PRESIDENT, SPECIAL INVESTIGATIONS, INC., AND LEGISLATIVE DIRECTOR, NATIONAL COUNCIL OF INVESTIGATION AND SECURITY SERVICES, NEW YORK, NEW YORK

Mr. HULME. Good afternoon, Mr. Chairman and Members of the Committee. My name is Bruce Hulme. I represent the National Council of Investigation and Security Services. I am a New York State licensed private investigator, having been so for 42 years. My company is Special Investigations, Inc.

As a profession that has been helping victims through the identity theft maze for years, our experience is that such thefts result from purloining of documents, files, charge slips, credit cards, and wallets, and according to the Javelin Strategy and Research survey, 47 percent of such theft is perpetrated by friends, neighbors, and employees.

We agree that additional measures can be taken to further reduce incidents of theft. Our concern is that some measures, unless amended, will have unintended consequences that would help create a safe haven for criminals and do substantial damage to the judicial system. We support Congressional efforts to protect data breaches. We favor limiting the use of the SSN on government documents, student IDs, and health cards. Certainly we do not believe that such information should be sold over the Internet to anybody willing to pay a fee.

However, we do have strong concerns with some provisions of H.R. 1745 and a Senate measure that would have direct and harmful effects on how our profession conducts lawful investigations by banning the sale of SSNs. The result would be that databases would not have accurate information about individuals and private investigators would be hampered in our efforts to locate individuals and perform many functions essential to the judicial system.

There are 46,000 American men named Bill Jones. Many of them have the same or similar dates of birth. Private investigators and others, of course, need to be able to differentiate between subjects for many purposes, including evidence in court proceedings.

One critical and effective tool used by private investigators is what is referred to as the credit header, that portion of a credit report that includes location and identifying information but discloses no credit data. That search is by far the most important one used by investigators when locating female witnesses. Women often change their names due to marriage and divorce, and it also helps to locate other individuals, particularly transients.

Pending legislation provides exceptions for law enforcement. This creates an obvious issue of due process because prosecutors with the full resources of the State will always have use of this tool while the accused would not. Database searches led directly to a witness or witnesses who recanted testimony and helped free a man wrongly imprisoned for 20 years. The same situation holds true in civil matters. Privacy legislation restricting the use of SSNs generally provides an exception for insurance companies, thereby creating an imbalance between insurance defense and plaintiffs' bars.

Investigators do not have access to a central criminal history database, as does law enforcement, so it is essential to develop ad-

dress information when seeking information about prior convictions so that we know what courthouses to go check out. In both civil and criminal trials, attorneys need to know the backgrounds of witnesses. We urge Congress that any restriction on the sale of SSN information include an exception to enable licensed private investigators and other State-regulated persons to conduct lawful investigations, including but not limited to identifying or locating missing or abducted persons, witnesses, criminals and fugitives, parties to litigation, parents delinquent in child support payments, organ and bone marrow donors, pension fund beneficiaries, and missing heirs.

Here are four quick examples of how we use SSNs. I was retained by the New York courts in a guardianship proceeding to recover \$300,000 in assets stolen from a 97-year-old retired Army officer. It was a successful result. The suspect pled guilty, was sentenced 3 to 9 years in State prison and ordered to pay \$360,000 in restitution and we got all the money back.

In San Francisco, a businessowner started getting statements in the mail saying he owed tens of thousands of dollars on computers and other equipment he never purchased. Someone had hijacked his identity, opened credit cards, store accounts in his name, set up a similar-type website in his name and his company's name. The police said they would only take a report, they wouldn't investigate. They passed it off to the Secret Service. His loss was \$80,000. The Secret Service said at that point, they had a \$100,000 threshold. A private investigator came into the case and with the use of credit header information found that an ex-employee, checking things out, had been using three names or several different SSNs and birthdates.

One of our association members reported a case that involved a woman who was left a sizeable inheritance by her uncle in the form of a trust. The investigator was able to eventually determine that she was recently married and living in Utah somewhere destitute, out of a pickup truck. That had a successful result.

A former president of our council testified just several years ago, I think, about a similar case before this Committee regarding a custodial parent whose child had been abducted 2 years prior. Her mother spent 2 years having a run-around with the police and politicians trying to get somebody to do the job. She went to this private investigator. Within basically minutes, running a credit header, determined enough leads as to where the husband might be, turned the information over to the police. They went there, got in, and the child was reunited with its mother.

As detailed in our statement, the association of regulators which regulates our profession, they support granting an exception for our industry in this, and we stand ready to assist the Committee in any way we can and thank you for this opportunity, Mr. Chairman.

[The prepared statement of Mr. Hulme follows:]

Statement of Bruce Hulme, Legislative Director, National Council of Investigation and Security Services, New York, New York

Good afternoon Mr. Chairman and members of the subcommittee. My name is Bruce H. Hulme and I am appearing today on behalf of the National Council of Investigation and Security Services (NCISS) where I serve as Legislative Director. I am past president and chairman of the Council and serve as a member of the Board

of Directors. I have been a licensed private investigator in New York for more than forty years and am president of Special Investigations, Inc.

We appreciate the opportunity to discuss how Social Security numbers can be used by perpetrators of identity theft, what Congress can do to mitigate the risk of such fraud, and the impact of pending legislation.

Social Security numbers (SSN's) have become the de facto identifier in the United States. The Social Security number is the single best way to distinguish among people of similar or identical names. That is why businesses have used SSN's on identity cards and customer records. It is also why SSN's are sought by those who wish to commit fraud, so they may attempt to establish an identity.

When Congress created the Social Security System nearly three-quarters of a century ago, it was not intended that the numbers issued to nearly every American would become the universal identifier for modern times. But that is what has occurred. An entire system of commerce is predicated on citizens being able to identify themselves based on this identifier. Unless each person has a viable substitute such as a password to take the place of the SSN, Congress should be very circumspect about eliminating the use of the SSN as an identifier.

Just as most commerce uses the SSN, the civil and criminal justice systems also require a means of identifying parties and witnesses in lawsuits and the commonality of dates of birth makes the SSN a necessary tool to be sure the courts have positive identification. It is true that some abuses have occurred by the misuse of the SSN, but the percentage of misuses pale in comparison to the number of positive uses applied every day in our economic and justice systems.

As a profession that has been trying to help victims through the identity theft maze for years, we applaud Congress' efforts to put additional laws on the books that will bring victims some relief. Recently enacted legislation should be of some assistance. The Fair and Accurate Credit Transactions Act included several identity theft provisions, and the 108th Congress adopted the Identity Theft Penalty Enhancement Act to increase sentences of convicted fraudsters. We were appalled to read recently that two caretakers who committed such fraud against their elderly patients received suspended sentences. Until the courts take the crime seriously, it will be difficult to deter such thieves.

Although a percentage of identity thieves no doubt gather their victims' identities from the Internet, our experience is that most such thefts result from the purloining of documents, files, charge slips, credit cards, and wallets from restaurants, stores, trash bins, the mails and private property. In fact, according to the Javelin Strategy and Research survey 47 percent of such theft is perpetrated by friends, neighbors or employees.

But we agree that additional measures can be taken to further reduce incidents of theft. Our concern is that some measures, unless amended, would have unintended consequences that could help create a safe haven for criminals and do substantial damage to the judicial system.

Publicity over data breaches for the past year have led to numerous bills in Congress and state legislatures to require that sensitive personal information, including Social Security numbers, be protected by those who hold it. Such breaches have occurred not only from data providers, but universities, banks and other institutions. Breaches have also occurred at every level of government. These breaches have been caused by lost computers, hacking, misplaced files and other means.

We support efforts to protect such sensitive personal data. Consumers should be informed when such data are divulged and should be provided assistance in order to protect themselves. And, businesses and other institutions holding such data have a responsibility to protect it.

With regard to Social Security numbers, we support limiting their use on government documents, student id's, health cards and other means of identification that could fall into the wrong hands. And we certainly don't believe that such information should be sold on the Internet to anyone willing to pay a fee. Many of these provisions are found in HR 1745, the Social Security Number Privacy and Identity Theft Protection Act.

We do, however, have strong concerns with provisions of HR 1745 and other measures that would have a direct and harmful effect on how our profession conducts lawful investigations. The Senate Committee on Commerce, Science and Transportation, for example, amended S 1408, the Identity Theft Protection Act, to effectively prohibit the sale of Social Security numbers with few exceptions. The result would be that databases would not have accurate information and private investigators would be hampered in our efforts to locate individuals and perform many of the functions essential to the judicial system.

How Private Investigators Use SSNs

As indicated earlier, the Social Security number is critical for determining identity. In past hearings, Lexis-Nexis has testified that there are 46,000 men in America named Bill Jones. Many of them have the same or similar dates of birth. Licensed private investigators need to be able to positively differentiate between subjects when rendering reports which will be used for many purposes including evidence in court proceedings. Behind any civil or criminal court case of consequence, you will usually find a licensed private investigator assisting the attorneys involved in such cases. The investigators are also then bound by the attorney-client privilege which adds a further measure of security to the information developed on individuals during the course of an investigation. Contrary to popular belief, most investigators work for law firms, insurance companies and corporations, not the general public.

One critical and effective tool used by private investigators is the "credit header," that portion of a credit report that includes location and identifying information but discloses no credit data. That search is by far the most important one currently used by investigators when locating female witnesses. Since women often change surnames over the course of their lives due to marriage or divorce, it makes it even more critical to be able to identify them by their SSN. The SSN does not change and allows us to locate these otherwise difficult to find witnesses. In California recently, database searches led directly to witnesses who recanted testimony and helped free a man *wrongly imprisoned for twenty years*.

In both civil and criminal trials, justice is served best by all parties getting access to all possible witnesses. Access to a fair trial is a fundamental right of American citizens. Without the ability to identify and locate all witnesses, that right is threatened.

The address information is used routinely to locate witnesses, particularly when they may be transient. Legislation restricting the use of Social Security numbers always provides exceptions for law enforcement. This creates an obvious issue of due process because prosecutors, with the full resources of the state, would have use of this tool while the accused would not. The criminal justice system needs balance. . . . the private investigator provides a counterpoint to the investigators in the public sector.

The same situation holds true in civil matters. Privacy legislation generally provides an exception for insurance companies, thereby creating an imbalance between the insurance defense and plaintiffs' bars in obtaining evidence in civil trials.

Investigators do not have access to the central criminal history database that law enforcement officials do, so it is essential to have addresses when seeking information about prior convictions. With prior address data, investigators know which courthouse records to search. This information is important for more than pre-employment purposes. In both civil and criminal trials, attorneys need to know the backgrounds of witnesses and potential witnesses.

Address information is valuable in locating stolen assets. I was retained by the New York courts in a guardianship proceeding to recover over \$300,000 in assets stolen from a 97-year-old retired Army officer by a neighbor caregiver. Through the use of credit headers I was immediately able to determine the identities and locations of the wrongdoer's relatives, properties and eventually their assets that had been taken from the victim. It was the initial header check on the suspect that uncovered an address in Myrtle Beach, South Carolina. That information developed leads that the victim's assets had been used to purchase expensive automobiles, real property in South Carolina and increased the bank account balances of the suspect. All under the guise that the 97-year-old victim, who was suffering from dementia, had given his life savings as gifts to the suspect. The suspect eventually pled guilty and was sentenced to three to nine years in state prison for second-degree grand larceny and ordered to pay \$360,000 in restitution to the estate of the victim, who, regrettably, died a month before sentencing of the defendant.

In numerous cases, such data have led to recovery of funds from persons not meeting their child support obligations. And missing persons, including abducted children, have been located with leads generated from credit headers.

It is no secret that law enforcement does not have the resources to respond effectively to most victims of identity theft. The crime is difficult to solve, and often involves several jurisdictions. So victims turn to private investigators for assistance.

Congress must consider that many licensed private investigators are former law enforcement officers and can assist the overwhelmed public law enforcement sector in fraud and identity theft related cases. Law enforcement is often under-manned and ill-equipped to deal with identity theft and usually violent crime cases take precedence. The victims then must turn to investigators in the private sector to as-

sist them in determining the extent of the fraud and the identity of the perpetrators. Investigators must have access to the necessary tools such as the credit header SSN search. Without access to this important investigative tool, it will become easier for criminals to shield themselves from discovery. They are fully aware of the limitations facing law enforcement.

Here is how SSN information helped solve one case: In San Francisco, an investigator reports working a case for a successful business owner who started getting statements in the mail saying he owed tens of thousands of dollars on computers and other purchases, none of which he knew anything about. He found someone had hijacked his identity, opened credit card and store accounts in his name and had even opened a web page mirroring his web page and had an e-mail address similar to his. The San Francisco Police said they would take a report, but would not investigate and suggested he go to the Secret Service. Although losses approached \$80,000, the Secret Service declined to take a report because losses had not reached a \$100,000 threshold. The victim hired a private agency. Using credit header information, they learned that the suspect, was an ex-employee with three aliases, three or four social security numbers, and three different dates of birth. The suspect was apprehended and prosecuted.

Such information is also valuable for locating lost heirs. One of our association members reported a case that involved a woman who was left a sizeable inheritance by her uncle in the form of a trust. The family had not had any contact with her for a number of years, so the attorney handling the trust asked for assistance. By using header information, the investigator was able to eventually determine that she was recently married and was living someplace in Utah. He was able to locate her husband's relatives and learned that she and her husband were destitute and living out of a pick-up truck in Oregon. He sent the requisite documentation to her in care of her husband's relatives and she rightfully obtained her substantial inheritance. Without access to header information, the investigator would not have been able to locate her.

A former president of our Council—NCISS—helped a custodial parent whose child had been abducted two years prior. The mother had spent those two years unsuccessfully trying to keep the police interested and writing various public officials seeking help. A credit header search revealed an address in Palm Beach, Florida, where the estranged husband had recently applied for credit. The police apprehended the husband and reunited the child with his mother.

One of our Texas members reports using a Social Security number "trace" to locate a female in need of assistance. A charitable fund had been set up to assist her with prenatal care and her childbirth. The credit header was an efficient means for the licensed investigator to quickly locate a needy person for charitable purposes at low cost.

Last year, NCISS met with members of the Federal Trade Commission to apprise them of the many ways private investigators rely on the SSN. We presented a dozen actual case examples of the sixty we had brought with us to that meeting.

We urge Congress to provide that any restriction on the sale of Social Security information include an exception to enable licensed private investigators and other state regulated persons to conduct lawful investigations, including, but not be limited to, identifying or locating missing or abducted persons, witnesses, criminals and fugitives, parties to litigation, parents delinquent in child support payments, organ and bone marrow donors, pension fund beneficiaries and missing heirs.

It is ironic that the end result of such well-intentioned legislation would be to make it more difficult to assist victims of identity theft and other frauds. It would make it less likely that the courts would hear from all relevant witnesses in both civil and criminal trials and less likely that stolen funds are recovered.

In conclusion, I would like to share with this committee the position of the International Association of Security and Investigative Regulators with respect to this issue. IASIR is an association of state and province regulatory agencies in the United States and Canada, having jurisdiction over a large part of the security industry and investigative profession. At their annual meeting last fall they passed the following motion:

IASIR acknowledges that regulated investigators are an integral part of the effective administration of justice, civil as well as criminal. In addition, state licensed investigators provide an essential service to the public, to businesses and government, and to the legal community for the purpose of preventing or investigating fraud including identity theft; reducing business losses such as embezzlement, robberies, burglaries, thefts, fires and other casualty claims; investigating workplace allegations including harassment, discrimination and other workplace risks; locating missing and abducted persons, witnesses, heirs, and deadbeat parents; as well as assisting in un-

covering significant misrepresentations or critical non-disclosures in conducting due diligence.

Since access to personally identifiable information is crucial to the welfare of many and often concerns not only individual physical safety but the protections of homeland security, IASIR recognizes and supports the necessity of those investigators, who are licensed and monitored by regulatory agencies, to maintain access to personal identifying information including but not limited to, social security numbers, dates of birth and driver's license numbers to assist in their important investigative mission.

NCISS stands ready to assist the Committee in its endeavor to protect consumer privacy without causing unintended consequences.

Chairman MCCRERY. Thank you, Mr. Hulme. Ms. Robinson, I am curious about one thing that we have discovered. According to the FTC, 61 percent of identity theft victims never contact the police department to report their identity theft. Do you have any idea why that is?

Ms. ROBINSON. Well, from my experience in working with victims, victims feel like the police don't care, and like the gentleman just said, the police will only take a report. They won't actively investigate the crime. They won't actively pursue the perpetrator.

Chairman MCCRERY. Does anybody else have a thought on that? Mr. Hulme?

Mr. HULME. Well, it is multiple jurisdictions that present problems. Law enforcement basically is just now starting to come up to speed. I can tell you from testimony I heard on the first panel that I probably investigated more ID thefts than the two government agencies. I know many of our members certainly have. I think it is a question of passing the buck, but it is definitely a major problem that has to be addressed.

Chairman MCCRERY. Thank you. Mr. Stein, you mentioned how financial institutions use SSNs as a tool to help verify the identity of their customers. Could you explain how, for example, a bank's customer identification program might work? What information do you request in addition to the SSN?

Mr. STEIN. Identity documents are always requested to prove up identity. The SSN helps as a determinant of an individual. As my esteemed colleagues have all represented about the Smiths, the Jones, and so forth, the SSN serves to identify the specific Jones or Smith that you are dealing with and to be able to tie those relationships, for example, together within a financial institution, to ensure that when you pull credit reports to determine creditworthiness for a loan, a mortgage, a credit card, you are actually receiving the information about the specific applicant who has applied to you so that you can make that credit worthiness decision appropriately.

Those are a number of ways in which that number is used. It is not used to verify identity per se. It is used to ensure that you are the Smith with whom we are dealing, and then we use your identity documents, typically a driver's license in today's society, and perhaps other pieces of identification, whether it be a passport, credit card, whatever, to confirm your identity.

The SSN itself doesn't confirm your identity in the absence of a CBSV or its predecessor, the Enumeration Verification System, where we have the ability to actually go out to SSA's database and

pull back or confirm the SSN, name, date of birth combination so that we know, in fact, we are dealing with the same person. In the absence of that, the number itself simply allows us to tie together disparate people using our disparate accounts that are using that same number as an identifier.

Chairman MCCRERY. Let us take Ms. Robinson's case, for example. Another Ms. Robinson stole her SSN, or got it, started using it, and applied for loans, evidently, and got them. Why couldn't that financial institution have just done a couple of extra things that might have raised flags and made them question the person sitting before them? She probably had a driver's license, that had her name which was almost the same, and it may have left out her middle initial, and that is not unusual, and so the person at the bank or the financial institution said, okay. Maybe then he should have looked at the address on the driver's license, and then surely the financial institution did a credit check. Maybe they should have compared the address on the driver's license to the address on her credit report, and when those are not the same, a flag goes up and you just either ask her there at the desk or call her back and say, there is a discrepancy in the address in your credit report. What is the deal?

Mr. STEIN. I have—

Chairman MCCRERY. Just a couple things. Why shouldn't you do that?

Mr. STEIN. I have two answers to that. The first one is, again, going back to the CBSV and the EVS system, had that been commercially available so that the financial institution could have verified the consumer's name along with the SSN and along with the date of birth, and assuming that the person who was misrepresenting her didn't have all three of those correct and documentation to support all three of those correct, the financial institution could have had an opportunity right there to have caught that. Number one, I would promote that the ability to verify that information is a key step in this entire process.

Now, not knowing exactly what the financial institution saw, and so I am—you have sort of asked me to second-guess what they did or didn't do here—but with respect to the credit reports that would be pulled based on the SSN and the name, I think that Mr. Pratt here has indicated the volume of address changes that happen in a year and the information tends to lag what gets into the credit reports, and so it wouldn't necessarily in and of itself as the sole trigger. The fact that the address wasn't in that credit report that represented the person in front of them wouldn't necessarily by itself have been a key indicator.

I also think that in a high-volume environment as card issuers deal with, it may also be difficult for them to find those really fine nuances between two people of the same name with the same SSN. I will tell you that had they been using a different name with her SSN, there would have been a warning that would have appeared on the credit report that would have indicated there is another name in the Bureau that is used sharing that same SSN. One of the problems is the very close similarity between the two names in this particular instance.

Chairman MCCRERY. Okay. Mr. Hulme, you have stated that your organization agrees that additional measures can be taken to reduce identity theft. You undoubtedly have a lot of experience in dealing with information resellers. Do you have any recommendations as to how they can improve their protection of SSNs, these resellers?

Mr. HULME. First of all, if there was a manner of getting a lot of the resellers—and I am not referring to the major ones, but two levels down or a level down—from selling this—pull this off the Internet and eliminate sales to the general public and you will eliminate 95 percent of the problems, in my opinion.

Chairman MCCRERY. Say that again?

Mr. HULME. I think one will eliminate 95 percent of the problems if sales of—

Mr. BECERRA. Could you repeat the whole answer? Pull it from the Internet—

Mr. HULME. Sure. Don't allow the sale of the SSN and personally identifiable information to be sold to the general public over the Internet. That would be my—I think that would be my first, strongest suggestion, and I heard one of the speakers earlier today say there were studies that maybe showed that. I can tell you that anecdotal information, and if you talk to most investigators and certainly our association, we think that if you pull down the sale of these items of personal information direct to the general public over the Internet, you will eliminate an awful lot of identity theft.

Chairman MCCRERY. Thank you. Mr. Levin?

Mr. LEVIN. Just one question. To sum up, how easy is it to steal identity?

Mr. HULME. Well, I am not a thief, but I would say—

[Laughter.]

Mr. LEVIN. I said how easy, not how.

Mr. HULME. Well, I think in some cases, the door is being left open. In some situations, I think there is the availability to get this information and it is being displayed often in areas where it shouldn't be displayed. The information obviously has to come off a lot of government documents, more than are necessary. The tons of mail that we get that get sometimes sent to the wrong place, even when it comes back to the Post Office, just check with the postal inspectors and you will find that they are now investigating quite a few crimes regarding what has been done with the mail that has been returned.

Mr. LEVIN. You are saying it is easy?

Mr. HULME. Yes.

Mr. LEVIN. Does anybody disagree with that?

Mr. PRATT. I don't think we disagree with that. I just want to emphasize, though, the point that has already been made, but just to drive it home, that fraud prevention systems are moving past the simple question of do you have a Social and a name that match up together. We discuss in our testimony different fraud prevention strategies that are being used today, and they really do have to do with bringing together disparate sets of information and attempting to foil the dilemma of having information which is far too openly sold out on the Internet, for example, by, for example, asking additional questions of the consumer that would probably not—that

the ID thief would not necessarily know. In an online environment, it might be to ask consumers additional questions that the thief probably wouldn't even know even if he or she had stolen a wallet.

Fraud prevention systems have clearly moved past the simple, do you have a set of data and have you matched it, yes or no, and we, too, agree that the SSA concept of matching information is a good one, but I suspect we would all agree that it is not the sum total of how you ultimately validate a consumer's identity. You may be able to validate that you have a real SSN, but then you are going to raise yellow flags. What about that address?

The Fair Credit Reporting Act, by the way, was amended in 2003 to obligate all lenders to have a system by which they will compare the old address or the address on the application with the address that you find in the credit report.

What about fraud alerts? The Fair Credit Reporting Act was amended in 2003 to obligate a lender to pay attention to the fraud alert, to make sure that it was actually processed, so that if one was placed on the file, that there would be additional contact measures taken to further authenticate the identity of the individual and attempt to foil the criminal from opening up new accounts.

I think those kinds of steps have been taken and that is why the world is a little different than even the last time I appeared before this Committee, when we talked about SSNs and the availability of them. Those are good steps along the continuum and the challenge is thieves become more clever and so, too, do the fraud prevention systems that have to stop them.

Mr. LEVIN. Thank you.

Chairman MCCRERY. Mr. Johnson?

Mr. JOHNSON. Thank you, Mr. Chairman. Mr. Pratt and Mr. Stein, I guess, you all haven't talked about how some companies will use the last four digits and some of them the first five, maybe, to identify people. Does that have any validity at all?

Mr. PRATT. From our perspective, again, Congressman, the Fair Credit Reporting Act stipulated that consumers could truncate SSNs when they order their credit report so that they could look at their credit report. For example, some laws attempt to do that.

Yes, there can be some strategies where I suppose truncation works. There are risks any time you start to truncate the number. For example, we actually have run data to show that even with the last four digits of an SSN, you can match up as many as 90 different Joneses in this country. You have to be careful. You have to be careful about when and where to employ a truncation strategy. In some kinds of database management systems, that is good. In some, that might not be so good.

Mr. STEIN. I think that one of the reasons that we use truncated SSNs is a layered approach for role-based access. If you segment a need around Social Security within a financial institution, there are three sets of needs. There are those people who don't ever need to see an SSN. You may have employees who, by virtue of their job role, have no need to ever see a customer's SSN, and by virtue of that role-based access, when they pull up information on the customer to respond to a question or whatever, they shouldn't see the customer's SSN at all.

There may be others within the organization who have a need to verify that as a component of the identity verification process, but they have no need for the full SSN. They don't need to know the whole thing for that consumer. A customer service center, for example, gets a phone call from Mr. Jones and one of the ways they may verify Mr. Jones in a remote environment is by having Mr. Jones tell them, or alternatively key into a voice response unit the last four digits of their SSN as a means to uniquely identify that Mr. Jones is the one for whom I am going to pull their account records. Again they have no need to see the full thing.

Then there are other employees within the organization who have clearly a need to work with the entire SSN, and that is a much, much smaller population. We are reducing the risk throughout that whole thing by taking it from the old world of financial institutions, where every employee saw every SSN, to a very small number who see a full SSN.

Mr. JOHNSON. Now, we tried at one time to get the military to change their procedure, but all of them use the SSN as an ID and it is on their ID card. Not only that, but my wife's ID card has both our numbers on it, not just one. Have you got any suggestions about how we can fix that problem, because that is an easy theft, I think.

Mr. PRATT. Congressman, all I can say is I think the world has changed enough that it is time to ask that question again of the military to see if they are willing to alter that system now.

Mr. JOHNSON. Okay. We can make them do it, I guess.

[Laughter.]

Mr. PRATT. It is true that every time the SSN is used on a medical identification card, when it is used on all the different places that it can occur, those are all risks that I think my colleague to the left has expressed are potential risks.

Mr. JOHNSON. Mr. Hulme, you are talking about people stealing your identity. I got stopped at the airport because they said I was a terrorist. Sam Johnson—there are a lot of them around.

[Laughter.]

They didn't have to have an SSN to verify who I was. They used other means. I think there is a way to get around that if we really want to and you all are probably doing as good a job as anybody. Have you got any suggestions on that?

Mr. HULME. No. All I can say is that some people definitely need to have access to that SSN. Along the same line, in fairness, it doesn't need to be laid out for the world to have.

Mr. JOHNSON. Yes. You are right. Thank you. Thank you, Mr. Chairman.

Chairman MCCRERY. Mr. Becerra?

Mr. BECERRA. Thank you all for your testimony. It is enlightening and also very disturbing. Ms. Robinson, let me ask you something. Have you cleared up your credit record yet?

Ms. ROBINSON. No, sir. As a result of Nicole Robinson using my data, one of the credit reporting agencies is still reporting her bad debt as mine.

Mr. BECERRA. Okay, stop. Mr. Pratt, you represent the credit bureaus.

Mr. PRATT. I do.

Mr. BECERRA. You hear Ms. Robinson saying that she has been going through this for years. Is there any reason why, if we contact you pretty soon, you can't tell us that the credit bureaus haven't taken care of Ms. Robinson's credit record?

Mr. PRATT. None whatsoever.

Mr. BECERRA. Okay. We will make sure that you get Mr. Pratt's phone number——

[Laughter.]

Mr. BECERRA. —and you will have——

Ms. ROBINSON. May I also add, though, that I have been dealing with that particular credit reporting agency for the last 4 years over the same problem, and it prevented me from getting a mortgage last year because they were reporting \$35,000 in bad debt that belonged to her.

Mr. BECERRA. Stop. Mr. Pratt said that you won't worry about that.

Ms. ROBINSON. Okay.

Mr. BECERRA. We will be in touch, and certainly you will be in touch with——

Ms. ROBINSON. Yes, I will be in touch.

Mr. BECERRA. Thank you, and Mr. Pratt, thank you for that. Mr. Stein, let me ask a question. What does Countrywide do with customers who, for whatever reason, close their accounts and their relationship with Countrywide. What do you do, what does Countrywide do with that personal private data that it has for that individual?

Mr. STEIN. There may be continuing obligations we have even after a relationship is closed, and let me speak more broadly for the financial industry in general because I think it is true whether lenders or financial institutions. There may be continuing obligations we may have with respect to that information that keeps it within the organization. That having been said, again, we talked about this role-based access and restricting the access to the information to those who have a true need so that you see only really that information which you have need by virtue of your job.

Mr. BECERRA. I have a mortgage through Countrywide. I pay it off. I no longer owe Countrywide any money. You have my SSN through the fact that I took out a mortgage with you. I no longer have any banking activity with you. You still maintain a file with my SSN?

Mr. STEIN. For our retention period, yes.

Mr. BECERRA. Which is how long?

Mr. STEIN. I believe it is probably either 5 or 7 years. Offhand, I don't——

Mr. BECERRA. Who has access to that?

Mr. STEIN. Again, it would depend on the specific job functions within an organization, but it would be those people who have, by virtue of their job function, a need to access it. For example——

Mr. BECERRA. Let me, because I am going to run out of time, so I don't want to do that, but let me ask you this. Would it be feasible economically for a company, an industry, to try to do more to shut down access to that personal data sooner than 5 to 7 years or make it much more restricted in terms of access to that informa-

tion, once there is no need to have an ongoing review of that information because the accounts, in essence, have been closed?

Mr. STEIN. Right, and I don't want to imply that once you close your relationship, the same people who have had access to that information when your relationship was open necessarily have it when your relationship is closed.

Mr. BECERRA. Okay.

Mr. STEIN. There is some population that does continue to have it, because you may call up a year later or 2 years later and have some question about your closed relationship that someone now needs to get access to.

Mr. BECERRA. Well, let me ask you this. If I were to call your toll-free number to check on the status of my mortgage 2 years after I have already finished and I punch in on the phone my old mortgage account number and I have some questions I need to have answered so I get an actual voice on the phone, would that person be able to pull up the information that would include the SSN?

Mr. STEIN. The answer is, it depends.

Mr. BECERRA. Okay. Don't go any further, because I will run out of time. If you can guide us on this, I think what we have heard is that we have got to try to limit the access as much as possible, but we also have to recognize that a lot of commerce depends on this information. Let us know what you are doing. What are the best practices that you are using to make sure that once you don't need it, you are not using it, and once you don't need it, others can't access it. It would be helpful to know who is doing a good job of making sure that we are closing the door on that information the quicker we can.

Mr. STEIN. Right.

Mr. BECERRA. That would be helpful. A hypothetical here. Social Security says, tomorrow, we are going to scrap the current SSN and the system that we have used. We are going to reinstate something totally different. Maybe it is with a number, but it is different. Everyone in America who has an SSN, you will be issued something else. At the same time, we pass a law saying we prohibit the use of this new Social Security identifier for anything other than Social Security. What do your industries, your agencies, what do you do?

Mr. PRATT. Beyond panic, I guess, would be the question.

[Laughter.]

Mr. PRATT. I think there are several parts to that answer. One, clearly, biometrics are being used in certain contexts and so, yes, there are even today—again, it is very important to distinguish between how the number is used to create an accurate database to say, I have data associated with this number and with this name together, versus how I am going to identify you and make sure that you are 100 percent who you say you are. Even today, consumers' acceptance of concepts like biometrics is much greater than it was perhaps a decade ago.

I think you would always find some sort of substitutes effect. I think the question is at what level of disruption in the system overall, between the time that you were to close off the system completely and then try to reinstate something else.

There would be, by the way, a legacy effect. All the data that was currently mediated by SSNs would remain. Court records would remain associated with the SSN. You are really talking almost generationally, anyway. You are talking about very, very long periods of time as you move away. It does get into discussions of cards and whether cards will have algorithms on them and whether cards will store additional information and whether they are used for limited purposes or more extended purposes. These are very complicated issues that certainly go well beyond the pale of our industry or, I suspect, any of us here at the table.

Mr. BECERRA. One way or the other, you will find some type of universal identifier that can help you keep tabs of the population.

Mr. PRATT. Well, I would say two things could happen. Number one, you could have less data mediated, which means, for example, consumers today who already are unhappy when we don't have a certain account that they have been paying on time for many, many years that Countrywide wants to use to approve a loan, when it is not in their credit report, they are also unhappy with us, just as they are unhappy when there might be data in their credit report that they say is not theirs. What you do have with the removal of an identifying system or a single unique identifier like the SSN is potential disintermediating and disconnecting data which can be mediated and which can be used for good things, such as me getting the car loan on the weekend or getting the student loan for my kids and so on and so forth. There are effects like that that we probably can't entirely predict today.

Even the FTC was asked to look at how SSNs interplayed with credit reports, and that was a study that was done during the 2003 FACT Act, and they concluded that, really, you move away from a binary, good or bad, proposition and you are on a continuum, move one direction, and maybe there is less SSNs and so maybe certain types of risks are reduced, but maybe you have disintermediated data. It was all about do you move toward more inclusivity or do you move toward more exclusion or separation? That is the kind of database continuum our members tend to operate on. Which way do I go?

Mr. BECERRA. Thank you.

Mr. STEIN. If I may just take one moment, when you talk about things like biometrics and other kinds of identifiers to uniquely identify an individual and you compare it to the SSN issue, the one thing to keep in mind is that the SSN is a national unique identifier. In the absence of having a national registry of fingerprints, retinal scans, facial recognition, hand geometry, whatever you want it to be, there is no way to take those disparate pieces and put them all together into a credit report. In the absence of that, it is probably more likely rather than less likely that the Nicole Robinsons of the world get joined with someone who really isn't them.

In this case, the person used her SSN with her same name. In other circumstances, you are going to have people, a whole bunch of Nicole Robinsons that may get joined together because there is not that unique identifier that puts them together.

Mr. BECERRA. Thank you. Thank you, Mr. Chairman.

Chairman MCCRERY. Thank you very much, gentlemen and ladies. We appreciate your testimony and your responses to our questions.

That concludes today's hearing. The Subcommittee is adjourned. [Whereupon, at 4:40 p.m., the Subcommittee was adjourned.] [Submissions for the record follow:]

Corona Del Mar, California
March 27, 2006

Dear Members of the Subcommittee and Participants of this series of Hearings: My name is John Patrick Kenney. I earn my living as a real estate developer and I am licensed as a real estate broker in California. I am a former recipient of Long Term Social Security of Disability Benefits. I am recent recipient of the National Republican Congressional Committee Ronald Reagan Medal and 2005 Businessman of the year Award. I am also the plaintiff in a Federal District Court Lawsuit against the commissioner of Social Security, currently awaiting a decision in case #SACV 05-00426 (MAN). John P. Kenney Vrs. Commissioner of Social Security. The agency misused my Social Security Number, identifying me as the recipient of a mistaken overpayment decision. This resulted in damages similar to those incurred in identity theft and was a violation of the bill of rights in the constitution of the United States. As I expect to win this case, actual damages today are approximately 12.5 million dollars and increasing at a rate of about \$30,000.00 per calendar day. Patrick O'Carroll, the SSA Inspector General has recently in this series and through reports, informed you, that the SSA may have made: 600,000 errors of overpayments and underpayments of the Social Security Benefits, has put you on notice of this, I'm sorry to say, error prone agency. The problem is that you, the congress, has backed this error prone agency with police powers to collect erroneous debts with minimal if any oversight. For example, the Federal Trade Commission is not permitted to enforce fair credit reporting or fair debt collection laws you enacted for our protection against the SSA. The president's management agenda is I believe correct . . . get our money out of the hands of this poorly managed bureaucracy. So, as a consequence of the above I legitimately expect a "Social Security" check soon between \$12,000,000.00 and \$20,000,000.00 depending on how long this agency wants to fight by withholding evidence, slander my character in the public court record, appealing to the 9th circuit or whatever failure prone tactic they may want to attempt. So . . . this error prone agency should not of and by itself and without real oversight possess the police powers have given it. I expect to prevail in my case and expect some public notice in the media to precipitate many an angry or scared taxpayer to contact you. What would happen to the general fund if 600,000 individuals had the opportunity, the inclination, the resources to sue the Social Security Administration for violating the privacy act as I have done? Please call on me if you need some help, even though I've missed meals and been forced by the above to try to relocate my business out of the country. I'm willing to help this subcommittee any way I am able.

John P. Kenney

Statement of J. Michelle Sybesma, Fishers, Indiana

You may find it hard to believe that once upon a time I carried an affidavit from the United States Postal Inspection Service verifying was indeed who I professed to be. From the looks of my photo, you might find it amusing to read my most recent state registered identification had said that I was not only Male, but of a Latin American heritage, 2 inches shorter, and about 15 lbs heavier than when I stood in front on you.

The truth was, before I figured out what happened I had a house in the low-income projects in Danville, IL and another just outside my hometown in Indianapolis, IN. Someone was utilizing my personal information and morphing it into someone that was in no way aligned with the principles of good ethics.

This was over ten years ago. I now know better than most what it takes to *establish new social security number and have to spend years in the fighting to reclaim your identity*. However, I am no victim. I am inclined to believe things happen for a reason and this happened to me so I might teach others how to prevent it. The

experience left me smarter, credit wiser and fighting mad to make sure it does not happen to others.

The most recent Federal Trade Commission statistics show that 12.7% of individuals surveyed have been personally touch by some sort of credit card fraud or identity theft.

As a consultant and professional speaker who covers topic to teach groups the importance of proper precautions to risk factors of Identity theft, I can tell you a more accurate statistic never stood.

If requested to testify, I can tell you a great deal about the inherent risk in business using our SSNs a primary identifier. Most people do not understand the long term impact this can have on the rise of this epidemic. Please consider contacting me to speak for your sub-committee. Not since the Fair Credit Reporting Act of 1996 has there been a piece of potential legislation that had such impact on that of Identity Theft. Thank you.



CMS Library

C2-07-13

7500 Security Blvd.

Baltimore, Maryland 21244



3 8095 00006545 4

